ソリューションブリーフ

アプリケーションアクセス管理（AAM）

認証管理の強化、効率化、および統合

認証はオンライン通信に不可欠なものです。クライアントとその通信相手の両者がお互いの身元を確認できる必要があります。E コマースの電子決済から、遠隔地間での医療診断、政府間の外交声明にいたるまで、ますます多くの遠隔やり取りが公衆のインターネットを介して行われる中で、当事者の身元確認は必須となっています。その一方で、大量のセッションが同時に発生すると、ネットワークやセキュリティのインフラストラクチャーが対応しきれなくなります。このため、当事者の身元を保証できること、エンドユーザーの使い勝手を高めること、強化されたデータセンターセキュリティの高まるニーズに応えるための拡張性という条件を備えたシステムを確立する必要があります。

認証に関する課題

組織はデータセンターのリソース保護の複雑さを解決する一方で、データ漏えいを防止する必要があります。内部や外部の Web ベースアクセスからクラウドサービス、BYOD（私物デバイスの業務利用）、およびソーシャルネットワークに至る現在進行中の移行の流れによって、管理者が IT セキュリティを監視する方法は大幅に難しくなりました。しかし従業員やパートナー、そして顧客やベンダーは、今ではますます多様化するアプリケーションに任意の場所から任意のデバイスを使用して安全にアクセスできることを求めています。多くの場合、これらは Oracle、SAP、SharePoint、Exchange などのミッションクリティカルなビジネスアプリケーションです。これらのアプリケーション資産への安全なリモートアクセスを可能にするには、厳格なネットワーク設計とセキュリティポリシーの強化が必要です。

アプリケーションサーバーなどのリソースを不正なアクセスから保護するには、組織は強力な認証を必要とします。このためには、ID ベースのアクセス制御を導入する必要があります。ID とアクセスの管理（IAM）ソリューションは、この必要なリソースの保護をサポートする一方で、規制の順守を保証します。この中核的な技術は、個別のクライアントにアクセスを許可すべきかどうかを判断するために使用されます。これらのソリューションは、カスタムのおよび標準化された内部アプリケーションと SaaS（Software-as-a-Service）アプリケーションもサポートしている必要があります。このようなソリューションを導入することは簡単ではなく、これらのソリューションを相互運用するには複数の要素が必要です。

IAM ツールの導入は、パズルのような認証ソリューションの一部分に過ぎません。このようなソリューションによって、エンドユーザーが過剰なネットワークリソースを消費しているのか、禁止されたプロトコルを実行してネットワークを誤用しているのか、または不適切な Web サイトにアクセスしているのかどうかが判別されます。しかし、このような複雑な処理タスクは大きな負荷をもたらす可能性があるため、これらのタスクを円滑に拡張することはできません。内部アプリケーションやエッジベースアプリケーションなど、数千に上る可能性のあるアプリケーションを対象にした認証を用意して構成することは、多大な労力を要する作業となる場合があります。IAM ツールは、それら自体が悪意のあるハッカー攻撃のターゲットとなる可能性があるため、保護される必要があります。継続的なアップタイムを保証する必要があるとともに、IAM リソースを将来のニーズに合わせて簡単に拡張できる必要があります。さらに、ユーザーの利便性を高めるためにはシングルサインオン（SSO）をサポートする必要があります。

課題

外部クライアントから Web ポータル、内部の機密リソース、およびモバイル /BYOD アプリケーションへのアクセス実現。ユーザーに意識させることのない、認証によるセキュリティ確保

ソリューション

A10 ネットワークスの AAM モジュールにより、IT 管理者は認証オフロードソリューションを導入可能。このソリューションは、A10 Thunder アプライアンス内に完全に統合されているため、一元化されたポリシーアクセス管理と容易な導入を実現

利点

- Webサーバーや AAAサーバーを認証処理の負荷から解放
- 複数の認証ポイントを統合して管理を簡易化
- 一般的な基本認証サービスとフォームベース認証サービスをサポート
- OCSPによってクライアント証明書を検証することでセキュリティを強化
- SAML 2.0に対応したシングルサインオン
- サーバーロードバランシングによりアップタイムを最大化しキャパシティを拡張
- 複数の保護レイヤーによってサーバーインフラストラクチャーを保護

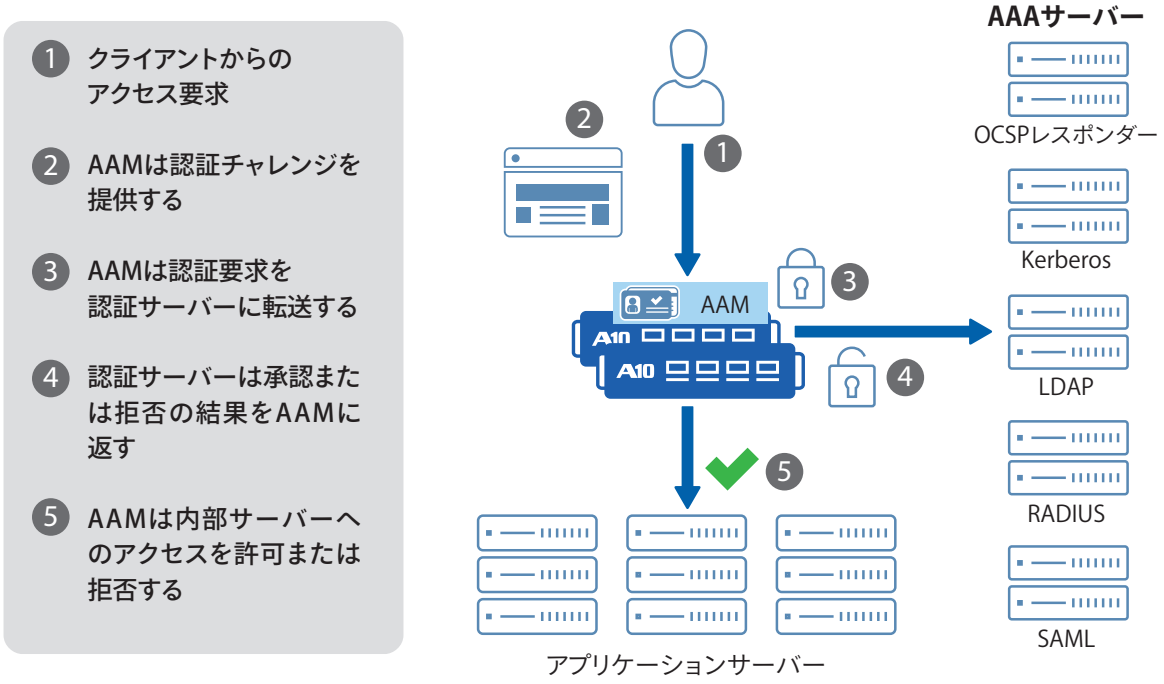

図1： RSAとA10による最適化された透過的なクライアント認証

A10 ネットワークスの AAM ソリューション：認証の一元化と保護

アプリケーションアクセス管理（AAM）モジュールを備えたA10 ネットワークスのA10 Thunder シリーズは、クライアント / サーバー間トラフィックに対する認証と承認を最適化して適用するための容易に導入可能なソリューションを提供します。AAM 機能は認証サーバー、ID データストア、およびアプリケーションとシームレスに統合して、ユーザーを認証してアクセス権限を適用します。AAM によって、A10 Thunder シリーズは Web サービスに対するエッジ認証ポイントとして機能します。多大な計算能力を必要とする多くの処理から IAM を解放することで、これらのようなツールは大幅に拡張されます。AAM は、SAML ベースの SSO や Online Certificate Status Protocol（OCSP）を含むすべての主要な認証スキームをサポートしているため、証明書ベースの認証によってモバイルデバイスおよびコンピュータのシームレスなサインオンが可能になります。既存のインフラストラクチャー内の複数の構成を変更する必要はありません。

AAM のシームレスな導入

A10 Thunder シリーズには統合された AAM 機能が搭載されており、データセンター内でこれらのアプライアンスが提供する他の豊富な機能と同じ場所に簡単に導入できます。A10 Thunder シリーズはアプリケーションの可用性、セキュリティ、および高速化のための多くの機能を提供し、これらのアプライアンスは、ネットワークの深部にある Web サーバー、アプリケーションサーバー、およびデータベースサーバーの近くに配置されます。AAM は、アプリケーションインフラストラクチャーを最適化するためのもう 1 つの手段に過ぎません。図 1 は、A10 の AAM ソリューションを既存の環境に簡単に統合する方法を示しています。Web ポータルへのアクセスであっても、オンライン財務取引などの機密用途、または内部ユーザーの認証が不要な可能性のある内部資産への外部アクセスであっても、この 5 段階のプロセスはシンプルなままです。

機能と利点

A10 の AAM ソリューションは、A10 ネットワークスの Thunder シリーズ用 OS Advanced Core Operating System（ACOS®）に含まれており、幅広い機能を使用して認証システムを最適化します。AAM は、インストールと構成のプロセスを効率化、設備コストと運用コストの削減、サーバーのアップタイム最大化、すべての主要な認証スキームのサポート、さらなるセキュリティレイヤーの追加、そしてシンプルなログインプロセスの実現により、これらのセキュリティの課題を解決します。

ネットワークの簡素化とコストの削減

- **認証の簡素化と統合**
  AAM テクノロジーを使用すると認証を一元管理することが可能なため、各 Web サーバー上に個別の認証ポイントを維持する必要がなくなります。複数の認証ポイントを統合することで、相互運用性と統合の問題が軽減されて、認証のポリシーとイベントを全社的な観点から捉えることができるようになります。この統合によって管理が効率化されるだけでなく、運用コストが削減されて、購入する必要のある SSL 証明書の数が減少することで、A10 Thunder シリーズの投資収益率（ROI）が高まります。

- **時間のかかるアプリケーション統合を不要に**
  組織全体のすべてのWebアプリケーションについてクライアント認証スキームをセットアップするには、コストがかかり長期にわたるWebサイトの更新が必要になります。A10 Thunderシリーズを利用して認証を行うことで、組織はアプリケーションコードの変更を回避できます。さらに、IT管理者が将来的に認証サーバーの置き換えを希望している場合は、すべてのアプリケーションを再コーディングする代わりにA10 Thunderシリーズの認証設定を更新するだけで済みます。

サーバーの可用性を保証

- **認証サーバーのロードバランシングでアップタイムと規模を最大化**
  A10 Thunderシリーズは認証サーバーへの要求をロードバランシングして高可用性を実現できます。サーバーのヘルスチェックによって、認証サーバーが稼働しており正常に応答することが確認されます。サーバーで障害が発生した場合は、A10 Thunderシリーズは認証要求を稼働中のサーバーに転送します。

- **Webサーバーと認証サーバーの負荷を軽減**
  認証処理には大きな負荷がかかるため、複数のサーバーが使用されている場合は、管理がより複雑になります。AAMはWebサーバーの負荷を軽減することで効率性を高めます。A10 Thunderシリーズは認証チャレンジをエンドユーザーに送信して、認証情報をAAAサーバーに転送して、承認された場合は、要求されたアプリケーションへのアクセスを許可します。

幅広い認証標準のサポート

- **幅広い認証スキームを容易にサポート**
  AAMがサポートしている一般的な認証サーバープロトコルとしては、LDAP（Lightweight Directory Access Protocol）、RADIUS、RSA SecurID、TDS SQL、Kerberos、クライアント証明書認証などが挙げられます。A10 Thunderシリーズは、OCSPレスポンダーに接続してクライアント証明書ステータスを確認できるとともに、Microsoft Active Directory（AD）サーバーに接続してSharePointとOutlook Web Accessのユーザーを認証できます。AAMは、フォームベースのログイン認証とHTTP基本認証の両方を管理できるため、組織全体にわたる柔軟な認証導入を可能にします。追加の認証リレーのための従来のWindows NT LAN Managerもサポートされています。

認証インフラストラクチャーのセキュリティ

- **サーバーインフラストラクチャーを保護**
  AAMはWebサーバーと認証サーバーに対する追加の防御レイヤーを提供します。AAMはすべての認証要求を代理送信することで、認証サーバーが直接の攻撃ターゲットになることを防止します。AAMは、許可されたユーザーのみにアクセスを許可することでWeb攻撃の攻撃対象領域を縮小します。したがって、攻撃者はパスワードで保護されたアプリケーションにアクセスできないため、Web攻撃を実行したりデータを盗んだりできません。事前認証がサポートされているため、複数の構成を変更することなく内部システムに安全にアクセスすることが可能になります。

ユーザーの利便性の向上

- **SAMLによるシングルサインオン**
  AAMはSSOを実現するためのSAML（Security Assertion Markup Language）をサポートしているため、ユーザーは1度認証されれば追加の認証なしで複数のアプリケーションとサービスにアクセスできます。A10 Thunderシリーズはサービスプロバイダーとして機能して、認証と承認をIdPのAAAサーバーに委任します。AAMは、複数のSAML 2.0ベース準拠IDプロバイダーと相互運用可能であることが実証されています。

- **SSOのための認証リレー**
  フォームベースのリレーによって、AAMはログインフォームに入力する機能をサポートしており、入力されたログインフォームは、A10アプライアンス上のユーザー認証情報キャッシュ内の情報を使用してAAAサーバーに渡されます。この機能によって、クライアント側でシングルサインオンが可能になります。ユーザー認証情報はADCアプライアンス上にローカルにキャッシュされ、新たな要求のためにクライアントが再認証されるときはこのキャッシュされた認証情報が使用されるため、それ以降に認証情報を再入力する必要はありません。このキャッシュはパーティションとVIPに対応しています。

複数の認証方式で実証された相互運用性

認証ログオン

HTMLフォームベース認証では、シンプルなHTTP/HTTPS要求を使用して、クライアントに対してアクセスに必要な認証情報（通常はユーザー名とパスワード）が求められます。認証のプロセスは次のとおりです。

- エンドユーザーはHTTPアクセス要求をサーバーに送信します。
- A10 Thunderシリーズは認証を行うための認証チャレンジ（WWW-Authenticateヘッダー）をエンドユーザーに送信します。
- フォームベースの認証を行うため、エンドユーザーのブラウザーにログイン画面が表示されて、ユーザー名とパスワードの入力が求められます。
- 入力が完了すると、ユーザーの認証情報が含まれた要求がA10 Thunderシリーズアプライアンスに送信されます。
- A10アプライアンスはこの認証情報を認証サーバーに転送して、エンドユーザー側で意識されない形で認証情報が確認されます。
- 認証に成功すると、認証サーバーからA10 Thunderシリーズに成功を通知するメッセージが送信されます。
- A10 Thunderシリーズは要求されたアプリケーションへのアクセスをエンドユーザーに許可します。

SAML 2.0ベースの認証

有力な標準として登場したSAML 2.0によって、セキュリティドメイン間で認証と承認の情報を安全に受け渡すことが可能です。このプロトコルは、認証と承認のデータをIdPとサービスプロバイダーの間で交換するためのXMLベースのオープンスタンダードです。SAML 2.0は、異なるサイトからであっても、すでに認証済みのクライアントに対してCookieを利用することでシングルサインオンを実現します。A10 Thunderシリーズは、サービスプロバイダー側で開始された認証とIdP側で開始された認

アプリケーションアクセス管理機能

認証方式

- HTTP 認証（基本、NTLM/Kerberos ネゴシエート）
- カスタム Web フォーム
- オプションの OCSP レスポンダーによる証明書認証
- SAML 2.0 サービスプロバイダー
  - SAML lite のサポート
  - ID プロバイダー（IdP）のサポート
  - サービスプロバイダーのサポート
  - バインディングのサポート：リダイレクト、ポスト、アーティファクト、SOAP
  - 認証要求、アーティファクトの解決、SSO のサポート

認証サーバーのサポート

- LDAP v2/v3
- Windows Integrated Authentication（WIA）
- RADIUS
  - RSA SecurID および Entrust IdentityGuard 認証エンジンのサポート
  - パスコード認証
  - 次のトークン / 新規ピンモード
- Entrust IdentityGuard
- Kerberos V5
- NTLM v2 または v1
- SAML 2.0 IdP
- OCSP（Online Certificate Status Protocol）
  - シングルサーバーまたはマルチサーバー認証のサポート
  - OCSP ステープリングのサポート
- データベースロードバランシング（DBLB）のための Active Directory サポート
- 状態監視のサポート

認証リレー

- 基本 HTTP
- Kerberos 認証
  - シングルサインオン
  - Kerberos の制約付き委任（KCD）
  - Kerberos プロトコル変換（KPT）
- NTLM
- WS-Federation
- フォームベースリレー（Exchange OWA など）または SharePoint

状態監視

- LDAP
- RADIUS
- Kerberos

負荷分散

- LDAP
- RADIUS
- OCSP
- Windows 認証サーバー

承認ポリシー

- ユーザーの承認ポリシーを規定するための承認ポリシーのサポート
- aFleX ベース承認のサポート
- SAML ユーザー承認
  - SAML 属性ステートメント認証のサポート
  - LDAP/RADIUS サーバー認証による SAML 認証

認証ログ

- パーティションレベルの認証ログ
- 設定可能な認証ログレベル
- syslog サーバーの認証ログのサポート

証の両方をサポートしています。次のプロセスは、サービスプロバイダー側で開始された認証を対象にしています。

- クライアントのアクセス要求が AAM の「サービスプロバイダー」に対して発行されます。
- AAM は SAML 認証要求を作成して、AAA サーバーに送信します。
- この要求が承認された場合は、クライアントは認証されて、サーバーはクライアントの ID と属性を示す SAML アサーションを作成します。
- このアサーションはデジタル署名と暗号化が施された上で、AAM に渡されます。
- AAM はアサーションの信憑性を確認して、その内容を復号化して要求されたアプリケーションとクライアント情報を共有します。
- アプリケーションはこのデータを使用してユーザーをサインオンさせて、SSO を可能にします。

OCSP（Online Certificate Status Protocol）

OCSP は、認証機関（CA）の公開された証明書失効リスト（CRL）を維持して、単一証明書の失効状態要求に応答するサービスです。この方法を使用して、受領されたクライアント証明書の状態を確認して、その証明書の信憑性をさらに保証します。AAM は OCSP をサポートしており、アプリケーションサーバーをこの処理から解放します。SSL クライアント認証の場合は、OCSP の認証サーバーは、A10 Thunder シリーズが提出済みクライアント証明書の失効状態を確認することを可能にします。状態が「有効」の場合、クライアントはサーバー上で構成されているリソースへのアクセスを許可されます。必要な認証プロセスはシンプルなものであり、次のステップで構成されます。

- クライアントから A10 Thunder シリーズに証明書が送信されます。
- A10 Thunder シリーズはその証明書の信憑性を確認します。
- OCSP レスポンダーから証明書の状態（有効、失効、または不明）が返されます。

豊富な管理ツールによるセキュリティの強化とインストールの簡素化

AAM の AAA ポリシーオプションは、きめ細かいアクセス制御を可能にすることでデータセンターのセキュリティを強化します。この結果として IT 管理者は、ユーザー、VIP、ACI、または要求された URL に基づいて独自に組み合わせた認証基準と承認基準を適用して、アクセスの許可または拒否が可能です。認証ロギング機能は、ユーザー認証の監査証跡を提供することですべてのアクセスを追跡することを可能にします。認証モジュールの開始、クライアントの要求と応答、セッションの作成と終了などのイベントは記録されて、自動アラートをセットアップできます。

AAM が提供するさまざまなテクノロジーにより構成を簡易化することが可能です。「デフォルトポータル」を通じて提供されている認証ポータル用の組み込みログインフォームは、そのまま使用することもカスタマイズすることもできます。A10 の ACOS には aFleX® が統合されており、認証と承認のカスタム要件をサポートします。このツールを使用すると簡単に、ユーザー名を変更または変換したり、ドメインを追加したり、複雑な承認条件ステートメントを処理したり、グループメンバーシップやロールなどのユーザー属性をバックエンドサーバーに送信したりできます。AAM はマルチテナント環境にインストールすることもできます。A10 Thunder シリーズは最大 1,023 個の独立したアプリケーションデリバリーパーティション（ADP）をサポートしており、これらの各パーティションは固有の AAM ポリシー構成をサポートできるため、導入の柔軟性が高まります。

まとめ― 認証管理の強化、効率化、および統合

組織はデータセンターのリソース保護の複雑さを解決する一方で、データ漏えいを防止する必要があります。内部や外部の Web ベースアクセスからクラウドサービス、BYOD（私物デバイスの業務利用）、およびソーシャルネットワークに至る現在進行中の移行の流れによって、管理者が IT セキュリティを監視する方法は大幅に難しくなりました。しかし従業員やパートナー、そして顧客やベンダーは、今ではますます多様化するアプリケーションに任意の場所から任意のデバイスを使用して安全にアクセスできることを求めています。多くの場合、これらは Oracle、SAP、SharePoint、Exchange などのミッションクリティカルなビジネスアプリケーションです。これらのアプリケーション資産への安全なリモートアクセスを可能にするには、厳格なネットワーク設計とセキュリティポリシーの強化が必要です。

次のステップ

A10 Thunder シリーズの AAM ソリューションの詳細については、A10 ネットワークスの担当者にお問い合わせください。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks は、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Web サービス事業者まで 7000 社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは 2004 年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界中のお客様にサービスを提供しています。
A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。
詳しくはホームページをご覧ください。

- URL：https://www.a10networks.co.jp/
- X（旧 Twitter）：https://twitter.com/a10networksjp
- Facebook：https://www.facebook.com/A10networksjapan

Learn More
About A10 Networks

お問い合わせ
A10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp

Part Number: A10-SB-19139-JA-02 JUN 2024