Always Secure. Always Available.

ソリューションブリーフ

ゼロトラストアーキテクチャ実現のためのリソースへのアクセス制御

多様なソリューションと連携する認証・認可ソリューション

ゼロトラストアーキテクチャの核となる認証・認可

組織の内部ネットワークと外部ネットワークの境界にファイアウォール等を設置し、組織の内部への侵入を防ぐ境界型防御はこれまで多くの組織で利用されてきましたが、ひとたび内部ネットワークへの侵入を許してしまうと被害が拡大しやすい問題が指摘されるようになりました。また、近年のリモートワークやクラウドサービス活用の拡大により、そもそも境界型でのセキュリティ担保が難しいことも問題となっています。これらの問題を解決するために、境界内のネットワークに存在するユーザーや端末・サービスを全面的に信頼して全てのリソースへのアクセスを許可するあり方を廃し、場所によって完全に信頼される（トラストな）状態を作らない（ゼロにする）構成であるゼロトラストアーキテクチャの実現が求められています。

ゼロトラストアーキテクチャの核となるのが、ユーザーや端末からの組織のリソースのアクセスに対して認証・認可を行うポリシー実行ポイント（Policy Enforcement Point；PEP）になります。組織の内部・外部問わず、全てのユーザーや端末・サービスからリソースへのアクセス要求が発生するごとに、その振る舞いや脅威情報などに基づいて動的に認証・認可を行うことでセキュリティを担保します。トラストな領域を作らず、また、同じユーザーや端末から同じリソースに対するアクセスであっても信頼し続けることが無いようにすることで、攻撃を受けた場合の影響を小さくできます。このように、組織のリソースに対するアクセスを適切に認証・認可する基盤の構築がゼロトラストアーキテクチャ実現において最も重要です。

多様なソリューションと連携する認証・認可プロキシ

A10ネットワークスのA10 Thunderシリーズが提供するアプリケーションアクセス管理（Application Access Management; AAM）機能により、A10 Thunderが多様なソリューションと連携した認証・認可プロキシとして動作し、組織内リソースへのアクセス制御を行うことで、ゼロトラストアーキテクチャにおけるPEPとして利用することができます（図1）。この機能を利用すると、A10 Thunderは端末やユーザーからのアクセスを受けた際に多様なID管理/証明書管理基盤と連携し、アプリケーションやリソースへの適切な認証・認可を行います。LDAP認証、RADIUS認証、Kerberos/NTLM認証などに対応し、外部の認証サーバーから取得したユーザー情報とユーザー属性に応じた認証と認可の制御が

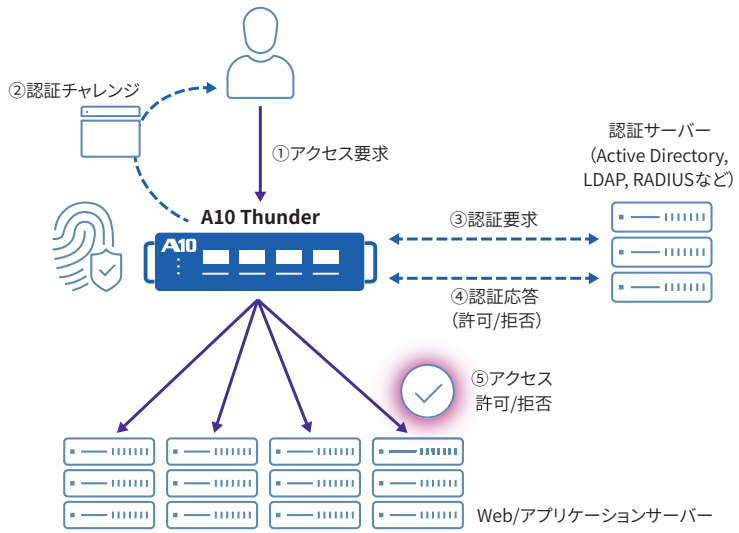

図1：A10 Thunderによるアプリケーションアクセス制御

課題：

- ゼロトラストアーキテクチャ実現の核となる、組織の内外にあるクライアントからのリソースへのアクセス要求に対する適切な認証・認可の実現
- 多様なID管理ソリューションと連携した適切な認証・認可の実現
- ボット等による不正なリソースへのアクセスの制御

解決策：

- A10 Thunderシリーズが提供するアプリケーションアクセス管理（AAM）機能による、リソースへのアクセスに対する認証・認可の実現
- SAML、RADIUS、LDAP、Kerberos、OCSP、OAuth2.0/OpenID Connectなどに対応した多様なソリューションとの連携
- 特許取得技術による、CAPTCHAを用いたボット等の不正なアクセスに対するアクセス制御

メリット：

- ゼロトラストアーキテクチャにおけるポリシー実行ポイント（PEP）としての利用
- Web/アプリケーションサーバーからの認証・認可プロセスのオフロード
- 認証・認可ポイントの集約による運用管理の効率化
- 柔軟なアクセス制御ポリシーの設定と詳細なアクセスログの取得によるクライアント/ユーザーの振る舞いの取得
- シングルサインオンや多要素認証への対応
- サーバー負荷分散やTLSオフロードを行うアプリケーション配信コントローラ機能やファイアウォール機能との併用による高可用性・セキュリティの強化・高いROIの実現

可能です。OCSP レスポンダと連携してクライアント証明書の有効性をチェックすることもできます。複数の認証サーバーの負荷分散を行うこともでき、NTLM 認証が出来なかった場合に LDAP 認証を行うなど、複数の認証方法へのフォールバックも可能です。SAML2.0 にも対応し、Service Provider（SP）として動作することで外部の Identity Provider（IdP）と連携して認証を行い、SAML アサーションによるシングルサインオンを実現することもできます（図 2）。OAuth2.0/OpenID Connect による認証・認可にも対応しており、パブリックな OAuth サービスと連携して、例えばソーシャルメディアでのアカウント情報などを利用した認証・認可を行うこともできます。認証・認可の結果や送信元・送信先等の情報を用いた柔軟なアクセス制御を実現できます。

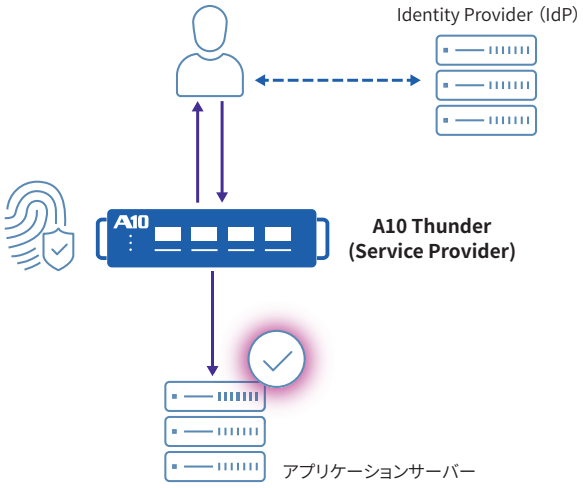

図 2：SAML 連携によるシングルサインオン

また、アプリケーションアクセス時のログインポータルで CAPTCHA と連携でき、ボットなどによるアクセスを制限することもできます。この CAPTCHA を用いたボットのアクセス制御に関しては、米国特許を取得しています（US20160330235A1）。

A10 Thunder が認証・認可プロキシとして動作することで、後段の Web/アプリケーションサーバーの認証・認可プロセスをオフロードできます。また、認証・認可ポイントを集約することで運用管理が効率化されます。認証・認可の結果を含めた詳細なアクセスログも取得できます。

認証サーバーとの連携はリバースプロキシとしての構成だけでなく、フォワードプロキシとして構成した場合も利用できます。これにより、組織内部から不特定多数のサービスへのアクセスに対しても同様に適切な認証・認可を実施できます。

ADC やファイアウォールと統合された機能

アプリケーション配信コントローラ（Application Delivery Controller; ADC）の機能やファイアウォールの機能が併せて利用できることも、A10 Thunder で認証・認可プロキシを実現する場合の利点となります。ADC の機能により HTTPS や HTTP/2 によるアクセスなどの SSL/TLS の復号処理をオフロードしたり、後段のアプリケーションサーバーの負荷分散や複数拠点に渡るグローバル負荷分散により高い可用性や高速なレスポンスを実現したり、Web アプリケーションファイアウォールや DDoS 攻撃防御機能によりセキュリティを強化したりすることが可能です。また、A10 Thunder CFW モデルを利用することで、ADC 機能に加えて L4 のステートフルファイアウォール機能を併せて利用でき、アプリケーションアクセスに対するセキュリティをさらに強化できます。最新の脅威情報がリアルタイムで提供される脅威インテリジェンスサービスなどと連携することで不正な IP アドレスからのアクセスなどを効果的に防御できます。

A10 Thunder は独自 OS や専用 HW を利用することで、コンパクトな筐体でも非常に高い TLS オフロード性能やサーバー負荷分散性能、ファイアウォール処理性能を有します。仮想インスタンスやコンテナにも対応しており、1 つのインスタンスで 100Gbps 以上のスループットを実現できます。また、これらの機能を 1 つの筐体で提供することで、ラックスペースや電力消費、利用するリソースなどが抑えられ、ランニングコストを抑えることができ、高い ROI に繋がります。

まとめ

A10 Thunder を利用することで、ゼロトラストアーキテクチャ実現の核となる、組織内のリソースへのアクセスに対する適切な認証・認可を実現できます。多様な認証方式や認証・認可ソリューションとの連携が可能です。アプリケーションサーバーから認証・認可のプロセスをオフロードでき、認証・認可ポイントを集約できます。A10 Thunder に集約された ADC 機能やファイアウォール機能との併用により高速なアプリケーション配信、高可用性やセキュリティ強化も併せて実現できます。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、サービス事業者やクラウド事業者および企業で利用される 5G ネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。A10 Networks 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拠地を置き、世界 117 か国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。

www.a10networks.co.jp/
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
a10networks.co.jp/contact

Part Number: A10_SB_AAM　Oct 2021