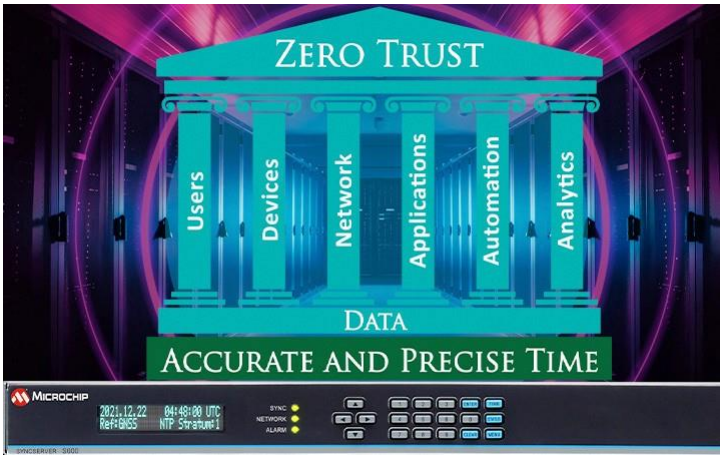
ゼロトラストデータセンターネットワークにおける信頼された時間とは何か、なぜそれが重要なのか？

概要

オンプレミスデータセンターやコロケーションデータセンターにZero Trust Architectureを展開する企業は、この分散ネットワークの正確な時刻同期とセキュリティに注意を払う必要があります。

タイムサーバーのセキュリティに注意を払う必要があります。正確な時刻は分散型ネットワークの運用に不可欠であり、ネットワークに接続されたタイムサーバーのセキュリティは、多くの点で信頼できるものでなければなりません。Microchip社製SyncServer S6x0は、正確な時刻を提供する能力だけでなく、Zero Trustの原則に準拠している点でも優れています。



なぜ時間が重要なのか

情報技術（IT）セキュリティは、分散したデータセンター内のデータ、リソース、個人情報などを保護する役割を担っています。その役割の一つは、すべてのネットワーク・アクティビティの「誰が、何を、どこで、いつ」管理し、組織のネットワークへの接続を許可されたすべてのデバイスを検証することです。

地理的に離れたデータセンターでは、ネットワーク活動の時間同期に関わる問題が発生します。データセンター間の非対称な経路遅延は、単一のネットワークタイムサーバーがネットワーク全体を同期させることを期待する場合、時間のオフセットをほぼ知ることができないことにつながります。時間のずれは、ログファイルのタイムスタンプの不一致につながり、ネットワーク管理システムの整合性を低下させることになります。

タイムスタンプの乱れを防ぐ

ネットワーク全体の時刻同期精度と、それがネットワーク管理とセキュリティに果たす重要な役割は、当然のことと思われがちです。

もし、すべてのデータセンターのすべてのネットワーク・デバイスが異なる時刻を持っていたらどうなるか、想像してみてください。組織内のネットワークは大混乱に陥るでしょう。ログとテレメトリーのタイムスタンプが相関しないので、ログファイルとネットワーク・テレメトリーは役に立たなくなる。例えば、リアルタイムで受信したシスログが、誤ってタイムスタンプされた場合、役に立たなくなる。

ダッシュボードに障害が発生するか、少なくとも不正確なデータが表示され、ほとんどの場合、アラームが発生します。重要なプロセスの開始が早すぎたり遅すぎたりする。ネットワークフォレンジックはほとんど不可能で、監査は無意味になり、ビデオのタイムスタンプは不正確になるなど、さまざまな問題が発生します。データセンター間の時間精度は重要であり、実際に重要なのです。

タイムソースの重要性

重要なのは、「誰が、何を、どこで、いつ」かを考えることです。いつ、どこで、誰が、どのように時刻を取得するのかを考慮することが重要です。

このとき、「誰が」「どこで」というのが単にタイムサーバーのIPアドレスがデータセンターの近くにあるインターネットのNTPサーバープールからのIPアドレスである場合、その情報の「いつ」に関して有効性と脆弱性を考慮する必要があります。

インターネットからの時間は、ゼロ・トラストのほぼすべての原則に違反しており信頼できる時間とは言えません。

信頼できる時間とは？

信頼できる時間とは、時間の正確さと正当性に関して、タイムサーバーが信頼されていることを意味します。また、タイムサーバーがネットワークに接続されたデバイスとして信頼され、企業のゼロトラスト・セキュリティ要件に準拠していることを意味します。

SyncServerが信頼できるタイムサーバーである理由。

SyncServerは、最も安全な信頼できるタイムネットワークデバイスとして、図1に示すように、ユーザー、デバイス、ネットワーク、アプリケーション、分析といったZero Trustモデル*の基本原則に適合しています。

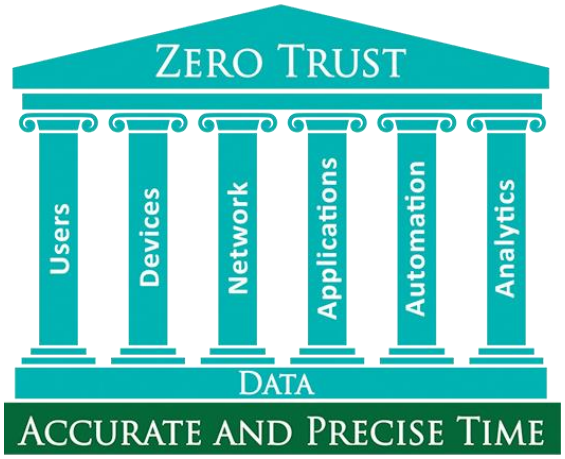


図1. 正確で精密な時間は、Zero Trustネットワークの根幹をなすものです

SyncServerは、NIST Special Publication 800-207: Zero Trust Architectureに記載されているコアコンポーネントにも適合しています。下記図2は、該当するコアコンポーネントを簡略化して表したもので、NISTが定義するデータプレーンとコントロールプレーンの間でSyncServerがどのように相互運用されるかを示しています。

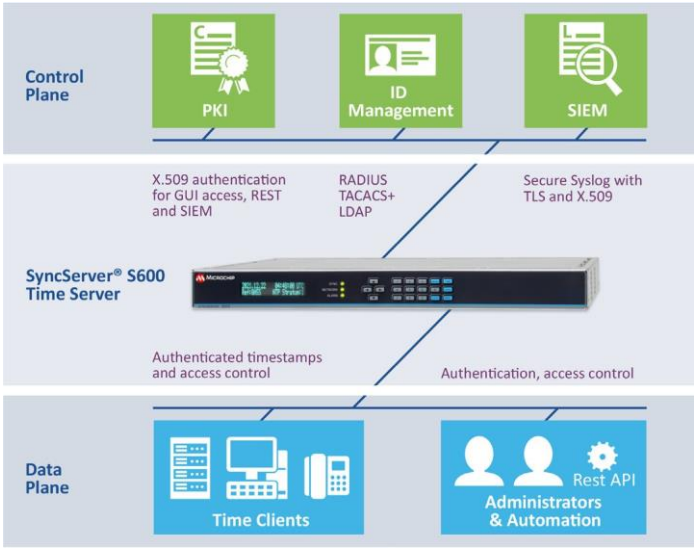


図 2. NISTが定義するデータプレーンとコントロールプレーン間のSyncServerの相互運用性

Zero Trustの前提として、時刻やタイムサーバーを含む全てのものに対して暗黙の信頼を与えないことが挙げられます。SyncServerを使用したZero Trustアーキテクチャで信頼できる時刻を実装するには、多くのケースが想定されます。私達はこれらのケースについて、インフォグラフィックを作成しました。各図では、SyncServer のセキュリティテクノロジーと関連する Zero Trust の柱が強調表示されているので、簡単に参照できます。すべてのインフォグラフィックは、Trusted Time for Zero Trust Networks の Web ページでご覧頂けます。

信頼された時間についてより詳しく知る

あなたの組織がデータセンター全体でZero Trustアーキテクチャに移行している場合、Zero Trustネットワークで信頼できる時間が非常に重要である理由を説明するアプリケーションノートが作成されました。この短い文書では、SyncServerがどのように時間のセキュリティを保証し、Zero Trustの原則に準拠するのかについて説明します。SyncServerのセキュリティ機能の詳細なリストと、それらがZero Trustモデルの要素とどのように整合しているかが記載されています。

SyncServer S600/S650 がネットワークのセキュリティ要件に適合しているかどうかを判断するために、企業のセキュリティチームは図 3 に示す参考チェックリストを使用することができます。

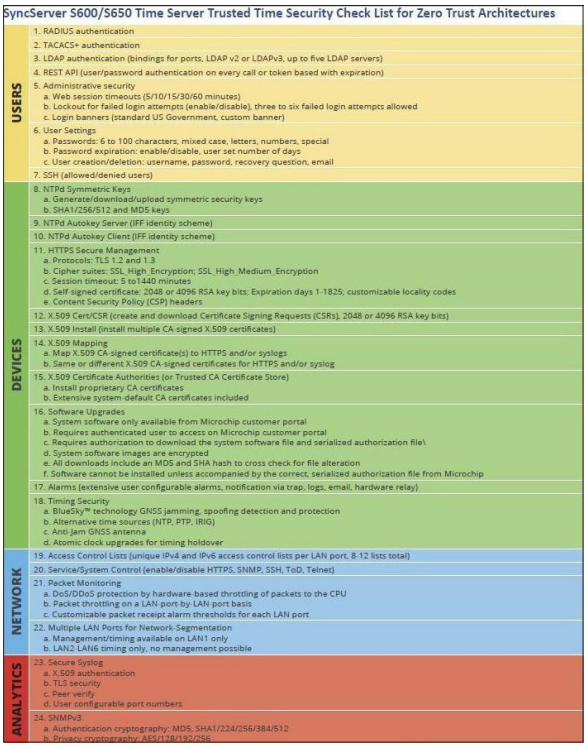


図 3. SyncServer S600/S650によるゼロトラスト実現に向けた各種チェックリスト

ゼロ・トラストタイムに適合するには

SyncServerは、最も安全な高信頼性タイムネットワークデバイスとして、地理的に分散したデータセンターにおけるZero Trust構想のサポートに最も適しています。時間とそのソースの安全性を確保し、Zero Trustの基本的な考え方に適合しています。

関連資料

ウェブページ: Trusted Time for Zero Trust Networks

アプリケーションノート: Trusted Time for Zero Trust Networks

* American Council for Technology-Industry Advisory Council (ACT-IAC), Zero Trust Cybersecurity Current Trends April 18, 2019