tufin The Security Policy Company.

実践ガイド ネットワークセグメンテーション

このガイドについて

このガイドは、効果的なネットワークセグメンテーション戦略を立て、実行したいと考えている組織に向けて記されています。リスク、コンプライアンス、セキュリティの戦略的目標と、その目標を達成するための方法を説明しています。また、ネットワーク・セグメンテーション・プロジェクトを成功させるために、よくある課題や避けられる落とし穴についても説明しています。

本ガイドは製品に依存せず、教育目的で作成されています。

ネットワークセグメンテーションについて

ネットワークのセグメンテーション戦略を考える際には、管理性や範囲が失われる可能性のある過剰なセグメンテーションを避けることも重要です。セグメント化は、コンプライアンス、セキュリティ、接続性などの大きな課題を解決するためのソリューションと見なされることが多いのですが、組織は管理性の現状を評価し、ネットワークを複雑にしすぎないように段階的に進める必要がある。セグメンテーションのアプローチが管理可能であれば、組織はゼロトラストの状態を追求するマイクロセグメンテーションと呼ばれる、より粒度の細かいアプローチを採用するでしょう。

セグメンテーションのメリット

ITガバナンスとリスク管理

セグメンテーションを、セキュリティポリシーを参照可能なベンチマークとして運用することで、既存のコンプライアンス違反を可視化し、コンプライアンス違反のアクセス要求を事前に特定することができます。効果的なリスクの識別と緩和（または例外の追跡）により、組織はポリシーの健全性を達成し、想定されるリスクの状態を把握し、IT ガバナンスを変更管理プロセスに組み込んで将来の変更を推進することができます。

コンプライアンス

セグメント化は、ネットワーク・セグメント間で許可またはブロックされるサービスを指定するアクセス・ポリシーで構成されます。これらのセキュリティポリシーをモデル化することで、コンプライアンスを確立することができます。許可されたサービスを通じた許容されるアクセスのベースラインを確立することで、組織はこれまでの違反を特定して是正し、新たな違反を未然に防ぐことができます。

ビジネス上必要とされることが、明示されたセキュリティポリシーと衝突することがあります。結果として生じる違反を例外として指定し、コンプライアンス違反を回避するために再認証のために追跡する必要がある。再認証プロセスにより、必要な接続性が確保され、例外に基づく非準拠のアクセスを考慮しないことによる監査の不注意な失敗をなくすことができます。

また、ネットワークセグメント間で参照可能なアクセスポリシーを確立することで、将来の意思決定の指針となる一貫したベースラインを提供します。ネットワークエンジニアリング（またはセキュリティ）は、組織内のナレッジリソースに頼るのではなく、自分に割り当てられたアクセス要求のコンプライアンスを迅速に評価することができます。コンプライアンスに準拠したアクセス要求は、設計、設定され、監査のために記録されます。コンプライアンスに準拠していないアクセス要求は、通常、拒否され、そのアクセス要求を期限付きの例外として提出するオプションがあります。コンプライアンスに反するルールが承認された場合、環境内の例外ルールは周知され、文書化され、再認証のために一貫してレビューされます。

このようなポリシーリファレンスの文書化とコンプライアンスモデルの作成を通じて、組織は何が「リスク」を構成するのかについてコンセンサスを得ることができます。あるネットワークゾーンにある機密データや重要資産を考えてみましょう。このゾーンは、別のゾーンへの接続を必要としますが、2つのゾーン間で安全と考えられるサービス、または安全性が低く脆弱性が高い可能性があるサービス（例：ポート22を介したTCP）についても注意する必要があります。セグメンテーションモデルでTCPを許可している場合でも、ルールの使用状況を監視し（急増した場合は侵害の可能性があるため）、使用されていない場合は、利用可能なポリシーから削除する必要があります。

セキュリティ

ゾーンを指定することで、企業は機密データの所在を一貫して追跡し、そのデータの性質に基づいてアクセス要求の妥当性を評価することができます。また、機密データの保存場所を指定することで、ネットワークやセキュリティの運用担当者は、より積極的なパッチ管理や積極的なシステム強化のためのリソースを割り当てることができます。

ゾーンを指定することでアクセスに対する監視を強化できるだけでなく、セグメンテーションを行うことで、アクティブな攻撃がネットワークに広がる前に隔離する論理的な方法を提供します。ゾーンとその間で許可されるサービスを指定することで、攻撃の際に悪用される脆弱なアクセス経路を特定し、緩和するための管理可能な方法を提供します。

セグメント化への準備

はじめに

組織は通常、実行可能な出発点を確立せずにセグメンテーション戦略に着手します。ITセキュリティは通常、ビジネスユニットやチームが存在するネットワークの場所を熟知しており、それらはしばしばゾーンとして指定されます。

しかし、大規模な組織でこれらのビジネス・エンティティーのそれぞれにゾーンを割り当てることは、最初から複雑すぎます。

最初の一歩を踏み出そうとしている組織では、初歩的なネットワーク・ゾーンを指定することが最も成功する方法であると考えられる。セグメンテーションを始めるための簡単なゾーンとしては、内部、外部、インターネット、DMZなどがある。これらのゾーンから始めれば、アクセスポリシーの改良が容易になり、最終的には受け入れ可能なポリシーを得ることができます。

ベースラインの策定

企業はまず、ゾーン間で許可されるサービスに関する標準的なポリシーに同意することから始める必要があります。また、セキュリティ・ポリシーが「コンプライアンス・ガイ」の頭の中に格納されているのであれば、ポリシー・ドキュメントの話し言葉の伝統から移行し、知識をエクセルやワードに書き写す時期に来ています。セキュリティ・ポリシーを文書化することで、記憶の欠落や予期せぬ病気のためにセキュリティ・ポリシーが修正されることがないことを保証するだけでなく、コンプライアンスのための最低限の参照可能なベンチマークを確立することができます。セキュリティ・ポリシーを文書化して一箇所に集中させれば、アクセス・ポリシーを修正するための各決定を一貫して自信を持って行うことができます。

コンプライアンス担当者が、ゾーン間で許可されるサービスの構成要素を十分に把握していない場合、ITセキュリティの専門家は、同僚と協力したり、技術的なリーダーシップに相談したりして、セキュリティ・ポリシー・モデルを作成することをお勧めします。もし、あなたが社内で唯一のITセキュリティ専門家であるならば、セキュリティ・ポリシーの策定に関するガイダンスを提供してくれる、この分野の既存のベンダーに連絡を取るべきです。既存のベンダーは、顧客に同様のガイダンスを提供している可能性が高く、あなたと共有できる反復可能なベストプラクティスを持っているかもしれません。

オーナーシップの確認

ネットワーキングデバイスやプラットフォームは、それぞれのベンダーが選択しています。これらのプラットフォームは、異なるビジネスユニットが異なる優先順位で管理することが多くなっています。パブリック・クラウドをコントロールするDevOpsなど）。）ハイブリッド・ネットワークでネットワーク・セグメンテーションを定義し、実施する準備をしているのであれば ハイブリッド・ネットワークでネットワーク・セグメンテーションを定義し、実施する準備をしている今、ネットワークの異なる部分のうち、どの部分が自分の管轄下にあり ネットワークのどの部分が自分の権限と所有権に属するのかを決定するのに最適な時期です。セキュリティ・インシデントが発生した場合には、各チームは セキュリティ・インシデントが発生した場合、各チームは侵害を抑制する責任を負いますが、ネットワークのオーナーシップを確立して初めて、セキュリティ・インシデントの正確な範囲を知ることができます。しかし、ネットワークのオーナーシップを確立して初めて、自分自身の説明責任と対応要件の正確な範囲を知ることができます。要件を知ることができます。多くの場合、この調査によって2つのチームが統一された目標に向けて調整され、ネットワークの接続性を改善する機会が得られます。ネットワークの接続性とセキュリティを向上させ、全員の利益につなげることができます。

オーナーシップの確認には、今後の新しいネットワークも含める必要があります。識別すると セグメント化に責任のあるネットワークの部分を特定する際には、採用または合併される可能性のある予想されるネットワークも含める必要があります。ネットワークの一部を特定する際には、既存のネットワークに採用されたり統合されたりする可能性のあるネットワークも含める必要があります。これにより このような変化がネットワーク・セグメンテーション戦略に影響を与えることを理解することで 新しいセキュリティの問題や、接続性を確保する上での障害となることを理解することで 考慮して計画を立てることができます。

管理性の確保

ネットワーク・プラットフォームの継続的な変化と平行して、ネットワーク・ポリシーの変化があります。お客様は クラウドファーストの取り組み、新規事業の立ち上げ、世界各地での新拠点の開設などが考えられます。新しいビジネスを立ち上げたり、世界各地に新しい拠点を開設したりするかもしれません。ネットワークがどのように変化しても、その変化を管理・追跡するには、一貫性が必要です。管理と追跡を一貫して行う必要があります。

“多くの場合、組織には、別のチームの担当者が使用している既存のツールや、以前に別の目的で購入した製品があります。以前に別の目的で購入した製品が、現在のセグメンテーションの目標に合致していることがあります。目標を達成するために 以前にネットワークで設定されたツールや、現在ネットワークの管理に使用されているツールを特定することで 識別することで、最初からセグメンテーション・プロセスの管理が可能になります。始めることができます。また、複数の既存のソリューションを見つけた場合は、それらを統合して、よりエンタープライズなソリューションを開発できないか検討します。
既存のソリューションが複数ある場合は、それらを統合して、継続的なセグメンテーション管理の設計、実装、および管理のための中央コンソールとして使用できる、よりエンタープライズに適したソリューションを開発できないかどうかを検討します。”

既存のツールがない場合は、社内のリソースに問い合わせて、基本的なものであれセグメンテーションの経験がある人を探し、それを基にツールを評価します。意外と見落とされがちなのが、ネットワーク・ソリューション・ベンダーに相談して、自社のツールを使ってネットワーク・セグメンテーションを管理するためのソリューションやガイダンスがあるかどうかを確認することだ。多くの場合、アカウント・マネージャーとの強固な関係は、製品購入の要件を超えたサポートを 製品購入の必要性を超えたサポートを受けることができます。

段階的な計画の策定

この段階では、どのようなリソースが利用できるのか、セグメンテーションの設計と実施に貢献できる人材はいるのか、セグメンテーションを技術的に実行するために利用できる外部の指導者はいるのか、といったことがわかります。これらの知識があれば、優先順位を見極めることができます。

まず第一に、ネットワークを高いレベルで評価し、どんなに初歩的に見えても、どのゾーンを指定したいかを検討します。ネットワークを半分に分割するだけでも、接続性の管理、アクセスの可視化、既存のアクセス・ルールに関連するリスクの特定が可能になる。また、内部、外部、インターネット、DMZの4つのゾーンを指定するという初歩的なステップを踏むことで、接続制限が不明な場合はその特定に着手することができ、さらにどのゾーンをセグメント化すべきか（機密データやサイバー資産など）の優先順位をつけることができます。

規制に準拠する必要がある場合は、センシティブ・データ・ゾーンを指定することから始めます（例えば、PCI DSSシステムおよびデータ用のゾーンなど）。このような細かいレベルから始めれば、コンプライアンスを念頭に置いた上で、一歩下がってより広いネットワークにアプローチすることができます。

いずれにしても、これらの初期ゾーンをさらにセグメント化することが望ましいでしょう（例えば、内部を機能別にセグメント化することができます）。このアプローチは、接続性の改善に対する理解を深め、アクセス削減を優先させ、機密データにアクセスするための攻撃を成功させるための特別な跳躍を義務付けるものです。そして、セグメンテーションの取り組みを続けていくうちに、より高度な粒度を実現する機会を得ることができます。VMWare NSX-TやCisco ACIなどのSDNソリューションは、マイクロセグメンテーションと呼ばれるセキュリティ・ファーストの考え方に基づいて、アプリケーションに対する個別のアクセス・コントロールを開発するための柔軟な方法を提供します。しかし、このように定義されたセキュリティ制御を適用するには、徐々に進めていく必要があります。なぜなら、セキュリティグループでこのような詳細な制御を行うと、個々のセキュリティグループが膨大になり、管理しきれなくなるからです。

セグメンテーションの落とし穴

過剰な取り組み

組織は、ネットワークに対するコントロールを強化するためにセグメンテーションを行うことがよくあります。しかし、あまりにも細かい粒度でセキュリティコントロールを確立すると、過剰なセグメンテーションになってしまいます。よくあるのは、一度に多くのことをやろうとしたり、最初からナノセグメンテーション（最も細かいレベルのアクセス制御を行うこと）という高い目標を設定したりすることです。

その結果、アクセスコントロールの変更を継続的に管理する際に、「分析麻痺」が発生します。500アプリケーションの環境で、すべてのアプリケーションにセキュリティグループを割り当てた場合、従来のセグメントに加えて、さらに500のセグメントが必要になります。また、ゾーンを再利用するよりも、アプリケーション・アクセス用に新しいセキュリティ・グループを作成する方が簡単です。膨大な量のゾーン このような方法で大量のゾーンを作成すると、チームは圧倒され、ゾーン間でセキュリティの優先順位を決めることができず、組織は複雑化した状態になります。

また、過剰なセグメンテーションの結果としてよく見られるのが、過剰に複雑なポリシーである。各ゾーンのポリシーは高度にコントロールされているため、組織は非常に特殊なアクセス要件に合わせてゾーンのポリシーを過剰に設計してしまうことがあります。このような粒度は、初期のポリシー要件を満たすものですが、セキュリティアナリストがコンテキストなしでポリシーを分析し、将来の変更を設計する必要がある場合には、すぐに圧倒されてしまいます。ポリシーを文脈なしに分析し、将来の変更を設計する必要がある場合、すぐに圧倒されてしまいます。

細分化は、ビジネスの安全性と有効性を高めるのに役立ちますが、アジリティの目標を阻害するほどの細分化を行ってはなりません。

情報に基づいて行動しない

セキュリティの世界では、自動化されたソリューションが膨大な量のアラートを送信しています。入力されたデータの量が、それらを処理し、優先順位をつけ、意思決定に利用する能力を上回ると、投資した時間とリソースが結果を出せなくなります。このシナリオでは、意思決定プロセスが破綻し、構築または購入したツールが棚ぼたになってしまいます。

ポリシー違反に対するアラート・メカニズムを設定できた場合、一貫性のある効果的な方法で対処するために、他のトリガーされたアラートと区別することが重要です。セキュリティポリシーへの違反は、例外として指定すべきかどうかを速やかに検討し、コンプライアンスを維持するための再認証に向けて追跡する必要があります。

コンプライアンスの測定にとどまらず、アクセス違反が意図的なものであり、適切なレビュープロセスを経て承認されているかどうかを評価することも重要です。セキュリティ専門家が APT の理想的な標的であることが多いことを考えると、違反行為をレビューするためのフラグを立てることは、コンプライアンス上重要であるだけでなく、攻撃者が認証情報を侵害していないことを確認し、機密データを含むネットワークゾーンへの攻撃を進めるために自分自身にアクセスを許可していることを確認するためにも重要なのです。

セグメンテーションの停止

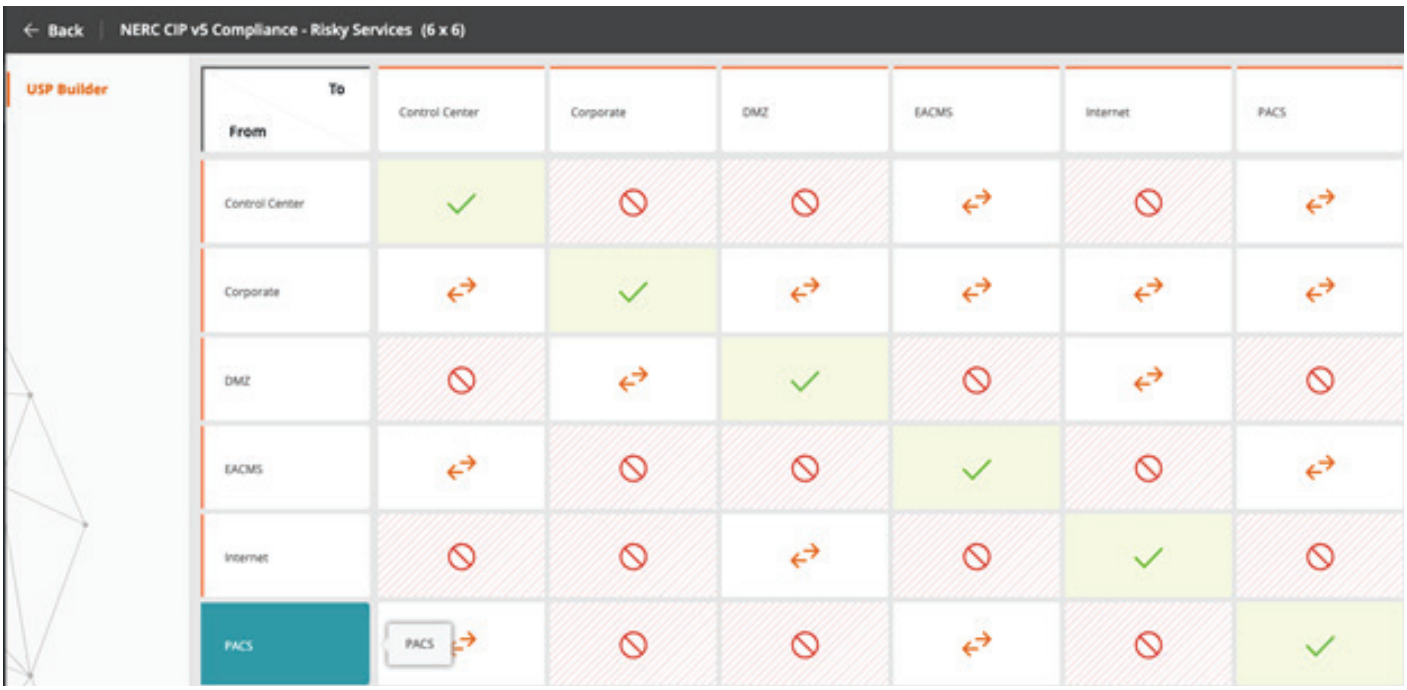
セグメンテーションは、完全な状態が定義されていない段階的なプロセスとしてアプローチする必要があります。ネットワークは変化するものであり、接続を管理するアクセス・コントロールも変化します。セキュリティは目的地ではなく、旅路である」という認識のもと、継続的なアプローチが最適です。セグメント化を段階的に管理可能なステップに分割することで、セグメント化を妨げることなく、競合するイニシアチブを並行して実施することができます。一歩前進すれば、見直し、修正し、その勢いを継続する機会が得られます。

あなたの会社は、ネットワーク接続を必要とする他のビジネスを買収したことがありますか？企業は、基本的なセキュリティ・ポリシーまたはベストプラクティスのセキュリティ・ポリシーを活用し、買収したネットワーク内で初歩的なセグメンテーション・モデルを適用して、リスクの現状を把握し、緩和策の優先順位を決定することがよくあります。その後、企業は買収したネットワークを独自のセグメンテーション・モデルで管理したり、既知のリスクの状態に問題がなければネットワーク・ゾーンを既存のゾーンに統合したりすることができます。

継続的なセグメンテーション戦略を維持するためには、クラウドなどの複数のプラットフォームを利用したり、ネットワーク・セグメンテーションの管理性を向上させるソリューションを将来的に購入したりすることも有効です。

Tufinのソリューション

“Tufinは、ゾーン間の接続マトリックスを提供し、どのネットワークゾーンを接続するかを決定するテンプレートから定義または選択し、2つのゾーン間で許可またはブロックされるポリシーを決定することができます。統一されたセキュリティポリシーにより、Tufin SecureTrackのユーザは、すべてのベンダとデバイスにわたるネットワークの可視化を開発し、許可されるサービスを定義することができます。コンプライアンスモデルに違反している既存のポリシーにはフラグが立てられ、例外として指定され、再認証のために追跡され、不要なポリシーは自動化されたワークフローによって削除されます。統一セキュリティポリシーは、変更管理ワークフローに統合されており、すべての変更にコンプライアンスを組み込み、ネットワークセキュリティチームがすべてのアクセスリクエストを確認する義務を軽減します。統一セキュリティポリシーは、ネットワークアクセスの変更要求を数日ではなく数分で完了させるための重要なソリューションです。
統一セキュリティポリシーは、ネットワークアクセスの変更要求を、数日ではなく数分で完了させるための重要なソリューションです。”



NERC CIPリスクのあるサービスに対するTufinの統一セキュリティポリシーマトリックス

Tufinについて

Tufin (NYSE:TUFN)は、何千ものファイアウォールやネットワーク機器、新興のハイブリッド・クラウド・インフラからなる、世界でも最大規模の複雑なネットワークの管理を簡素化します。企業は同社のTufin Orchestration SuiteTM を選択することで、強固なセキュリティ体制を維持しつつ、刻々と変化するビジネス需要に対応するための俊敏性をもたらします。

Tufin Orchestration Suiteは、攻撃対象を減らし、安全で信頼性の高いアプリケーション接続の可視性を高めたいというニーズに応えます。設立以来、2000社以上のお客様にご利用いただいているTufinのネットワーク・セキュリティ・オートメーションは、企業が数日ではなく数分で変更を実装することを可能にし、セキュリティ態勢とビジネスの俊敏性を向上させます。詳しくは www.tufin.com をご覧ください。

Tufin, Unified Security Policy, Tufin Orchestration Suite and the Tufin logo are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Copyright © 2021 Tufin
TD20210307-20210801