VMware NSX for Horizon

概要

VMware NSX™ for Horizon® は、仮想デスクトップ インフラストラクチャ（VDI）のネットワークにスピードとシンプルさをもたらすソリューションです。ネットワークのプロビジョニングに時間をかけることなく、仮想デスクトップに動的に適用されるポリシーを数秒以内に作成できます。また、データセンターから、デスクトップやアプリケーションまでセキュリティ ポリシーを拡張し、業界をリードするセキュリティ ソリューションとも連携できるため、拡張性の高いプラットフォームの構築が可能です。

メリット

- データセンター内のワークロードに隣接する仮想デスクトップのセキュリティを強化
- 論理グループ、ロール、またはタグを使用して、ユーザーのネットワークポリシーとセキュリティ ポリシーの管理を簡素化および迅速化
- デスクトップが作成されると同時にポリシーを適用し、基盤となるインフラストラクチャを問わず自動的に仮想マシンにも適用
- 業界をリードする、アンチウイルス、マルウェア対策、侵入防止、および次世代のセキュリティ サービスと連携

仮想デスクトップとアプリケーションのための ネットワークとセキュリティ 迅速性、拡張性の向上と複雑性の軽減

デスクトップとアプリケーションの仮想化により、クライアント コンピューティングのセキュリティ強化と優れたエンタープライズ モビリティを実現できるほか、デスクトップとアプリケーションを統合管理することで、保存されたデータの保護、アプリケーションへの不正アクセスの防止、およびイメージのパッチ適用、メンテナンス、アップグレードの効率化が可能です。

ただし、デスクトップとアプリケーションの仮想化により、データセンターのファイアウォールの内側では、数百台から数千台ものデスクトップがほかのユーザーやミッションクリティカルなワークロードに近接して配置されているため、マルウェアなどの攻撃を受けやすくなるという、新たなセキュリティに関する課題も生じます。このような攻撃はデスクトップからサーバへと広がり、データセンターの広範囲にわたり、East-West トラフィックへの脅威は、現在多くのお客様に影響を及ぼしています。特に、セキュリティとコンプライアンスについて厳しい要件があるお客様には深刻な課題です。

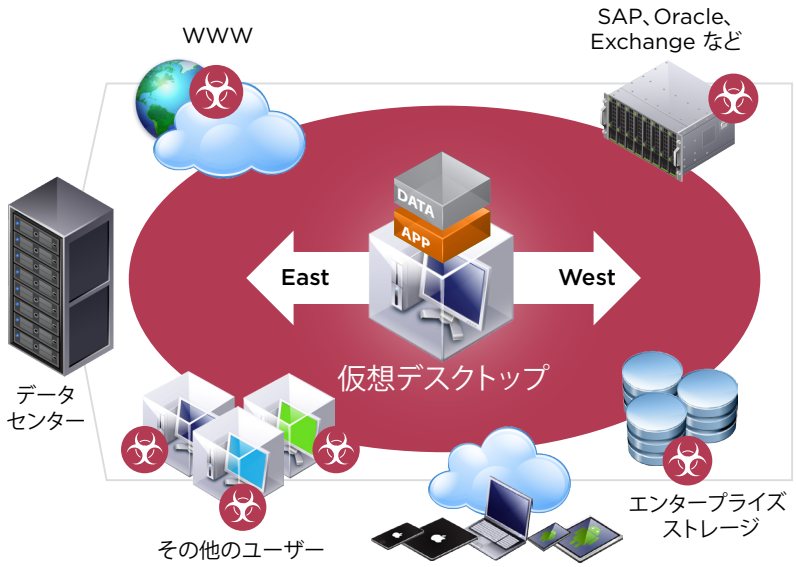

図 1： データセンター内における East-West トラフィックのセキュリティの問題

ユーザーやワークロードに永続的に適用されるネットワークおよびセキュリティ ポリシーを管理するために、これまでハードウェア中心のアーキテクチャに多大な投資が行われてきましたが、このようなアーキテクチャは、設備投資コストが高額なうえ操作が複雑で、変化し続けるビジネス環境に適応するには俊敏性が欠如していました。

VMware NSX for Horizon

VMware NSX for Horizon では、データセンター内の East-West トラフィックを効果的に保護すると同時に、ネットワークおよびセキュリティ ポリシーを迅速かつ容易に管理することが可能です。また、インフラストラクチャ、デバイス、および場所を問わず、エンド ユーザーの仮想デスクトップとアプリケーションにポリシーを動的に適用することができます。

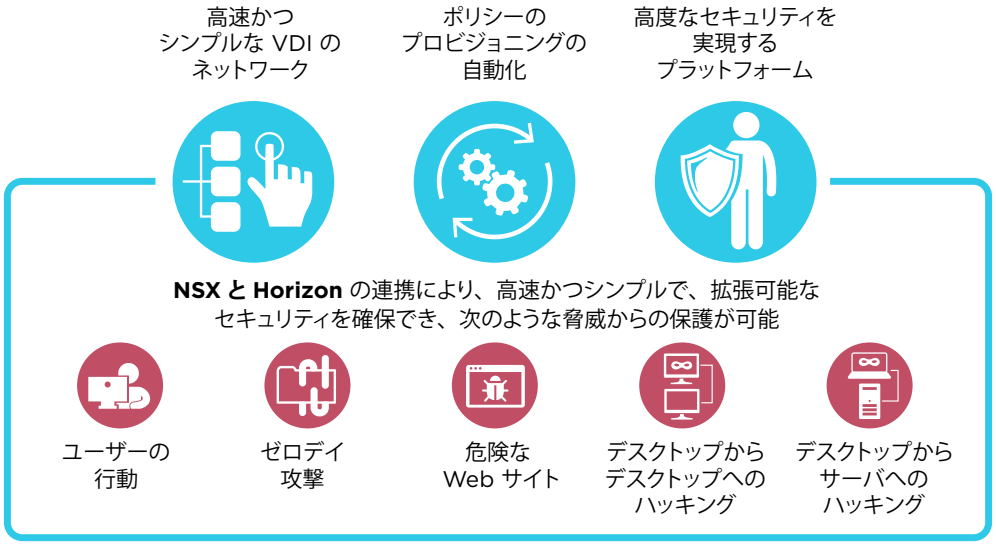

図 2：NSX for Horizon による、迅速性、拡張性が向上し複雑性が軽減された VDI のネットワークとセキュリティ

高速でシンプルな VDI のネットワークとセキュリティのメリットを実現できるこのソリューションでは、ネットワークのプロビジョニングに時間をかけることなく、仮想デスクトップに動的に適用されるポリシーを数秒以内に作成できます。

また、セキュリティ ポリシーをデータセンターからデスクトップやアプリケーションに拡張するとともに、業界をリードするセキュリティ企業の製品と連携する、拡張可能なプラットフォームを提供することから、デスクトップ全体のセキュリティを徹底して保護することが可能です。

VMware NSX for Horizon の仕組み

VMware NSX for Horizon はデスクトップ仮想化のセキュリティを強化し、管理者が統合的にポリシーを定義できるようにすることで East-West トラフィックの脅威からの保護を支援します。定義されたポリシーはすべての vSphere ホスト内のハイパーバイザー レイヤーに配布され、デスクトップが作成されるとすぐに各仮想デスクトップに自動的に適用されます。データセンター内の仮想デスクトップと、隣接するワークロードを保護するには、VMware NSX のマイクロ セグメンテーションを実装することで、各デスクトップの境界が保護されます。また、このセキュリティは、VMware NSX の分散仮想ファイアウォールの機能を使用して、各仮想マシンが送受信するトラフィックを監視し、デスクトップと隣接するワークロード間の不正アクセスを排除するほか、仮想デスクトップをほかのホストやほかのデータセンターに移動させると、デスクトップの移動に伴いポリシーも自動的に追従します。

機能とメリット

VMware NSX を Horizon 環境に導入することで、デバイスや場所を問わずエンドユーザーに動的にセキュリティ ポリシーを適用しながら、迅速かつシンプルな仮想デスクトップ インフラストラクチャ（VDI）のネットワークを実装することが可能です。

高速かつシンプルな VDI のネットワーク

VMware NSX for Horizon では、数回クリックするだけですべての仮想デスクトップに対するセキュリティ ポリシーを作成、変更、および管理できます。セキュリティ ポリシーをユーザー グループに迅速にマッピングすることができるため、仮想デスクトップを迅速に導入することが可能です。また、スイッチ、ルータ、ファイアウォール、ロード バランシングなどの仮想ネットワークの機能を展開できることから、VDI 用のネットワークを容易に構築できます。複雑な VLAN、ACL、またはハードウェア構成の構文は不要です。

エンド ユーザーとデスクトップにポリシーを動的かつ自動的に適用

ネットワーク セキュリティ サービスによって、エンド ユーザーのコンピューティング環境に動的に適応するポリシーを設定できます。ネットワーク セキュリティ サービスは、ロール、論理グループ、デスクトップのオペレーティング システムなどの要素に基づいてユーザーにマッピングされ、基盤となるネットワーク インフラストラクチャには依存しません。デスクトップが作成されると同時に、統合管理されているポリシーが各デスクトップ仮想マシンに自動的に適用されます。データセンター全体の仮想デスクトップに対してセキュリティが永続的に確保されるため、環境を確実に拡張できます。

高度なセキュリティを実現するプラットフォーム

VMware NSX は、豊富な実績を持つセキュリティ パートナーが提供する業界最高クラスの製品と連携することで、拡張性の高いプラットフォームを提供します。サービスを動的に追加することにより、仮想デスクトップのセキュリティを、データセンターからデスクトップやアプリケーションに拡張することができます。Trend Micro 社、Intel Security Group 社、および Palo Alto Networks 社をはじめとするパートナー各社が提供する、アンチウイルス、マルウェア対策、侵入防止、および次世代のセキュリティ サービスにより、オペレーティング システムやブラウザ、E メールなどの保護が可能です。

詳細情報

Horizon および VMware NSX の詳細については、VMware の Web サイトをご覧いただくか、Twitter をご参照ください。

VMware Horizon のリソース

製品ページ：http://www.vmware.com/jp/products/horizon-view/

ブログ：http://blogs.vmware.com/euc/（英語）

Twitter：@VMwareHorizon（英語）

VMware NSX のリソース

製品ページ：http://www.vmware.com/jp/products/nsx/

ブログ：http://blogs.vmware.com/networkvirtualization/（英語）

Twitter：@VMwareNSX（英語）

vmware

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp

アイテム No.：4461-VMW-SB-NSXNETWKSECUR-A4-20150401