

データセンター ネットワーク向けの包括的なセキュリティ

企業のデータセンターには、従業員、顧客、外部関係者に関する機密情報、知的財産、重要なビジネス情報などの資産が保管されています。またユーザは、社内だけでなく社外からのアクセスも含めて、さまざまなデバイスとアクセスポイントを利用して企業データにアクセスしています。データセンター インフラストラクチャのセキュリティを強化し、規制に準拠し、保管されているデータはもちろん伝送中のデータを保護することは、ネットワーク管理の課題でもあり、技術的な課題でもあります。データセンターを保護するには、ネットワーク インフラストラクチャからコンピューティング アプリケーションに至るまで、すべてのレベルで統合されたポリシーが必要です。安全性の高いネットワーク ファブリックは、データセンターの保護に大きな役割を果たします。Cisco Nexus 7000 シリーズは、次世代データセンターに必要とされるインフラストラクチャ セキュリティを提供します。

Cisco® Nexus 7000 シリーズ スイッチは、ミッションクリティカルなデータセンター運用のための、スケーラビリティの高いエンドツーエンドの 10 ギガビット イーサネット スイッチ シリーズです。ファブリック アーキテクチャは 15 テラビット/秒 (Tbps) を超えるトラフィック レベルに対応でき、将来は 40 Gbps および 100 Gbps イーサネットをサポートします。このプラットフォームは、最先端のモジュール型オペレーティング システムである Cisco NX-OS で動作し、優れたスケーラビリティ、継続的なシステム運用、サービスビリティ、およびデータ転送の柔軟性を実現できるように設計されています。Cisco Nexus 7000 シリーズは、堅牢なコントロール プレーンおよびワイヤレートの暗号化と復号化によってサポートされる包括的なセキュリティ機能を提供します。これにより、データセンター内で使用されるプロトコルやアプリケーションにとって複雑さが軽減され、より透過性の高いセキュリティ制御が可能になります。

Cisco Nexus 7000 シリーズによるデータセンターのセキュリティ サポート

- **Cisco TrustSec**: 独立した組み込みのハードウェアおよびソフトウェア機能を通じて提供され、デバイス アドミッション コントロール、セキュリティ グループベースのポリシー、およびリンク層での暗号化を可能にします。
- **統合型セキュリティ**: データセンターのネットワークとデバイスを保護します。
- **IEEE 802.1x**: 認証および許可で使用します。
- **ポート ACL (PACL)、ルータ ACL (RACL)、VLAN ACL (VACL)、およびロールベース アクセス コントロール (RBAC)**: 権限のセキュリティを保護して、情報の保護を柔軟に行えるようにします。

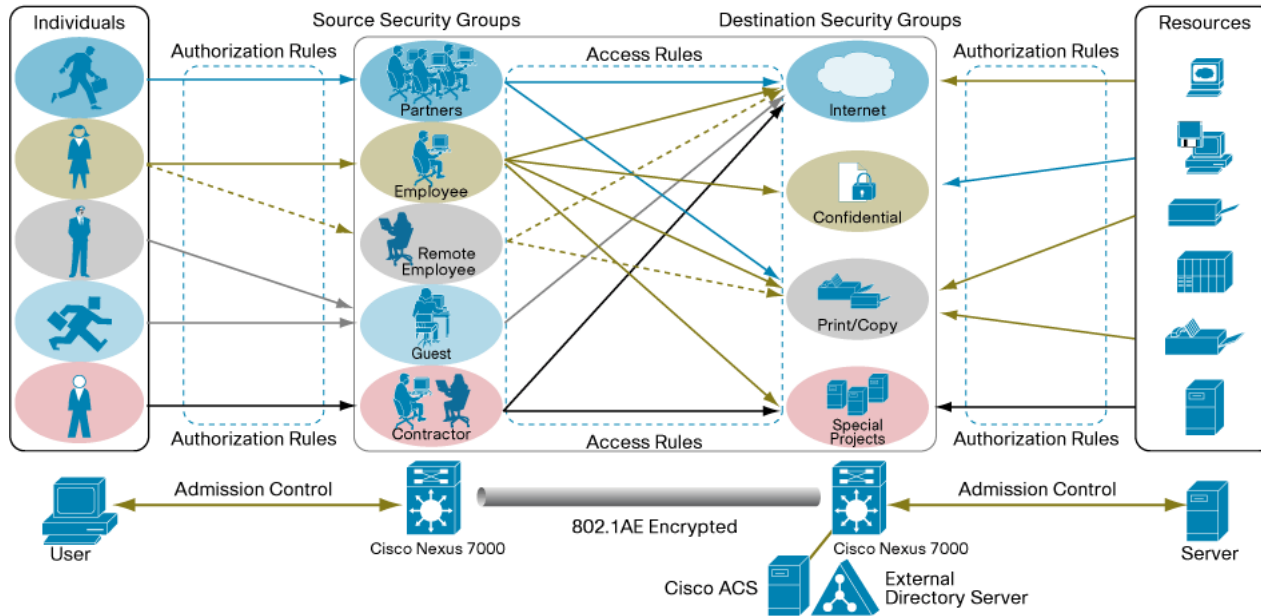
- **コントロール プレーン保護**: ハードウェア ベースのポリシー設定により、強化されます。

Cisco TrustSec

Cisco TrustSec は、アドミッションおよびアクセス コントロール用の機能の豊富なポリシーベースのサービスであり、これによってパケットの機密性と完全性がネットワーク ファブリックに組み込まれます。Cisco TrustSec は、IEEE 802.1AE 標準に基づく Security Group Tag (SGT; セキュリティ グループ タグ) を使用し、ネットワーク上のどこからでもロール情報にアクセス可能な、ロール対応のネットワークを構築します (図 2 を参照)。Cisco Nexus 7000 には、次のような機能が組み込まれています。

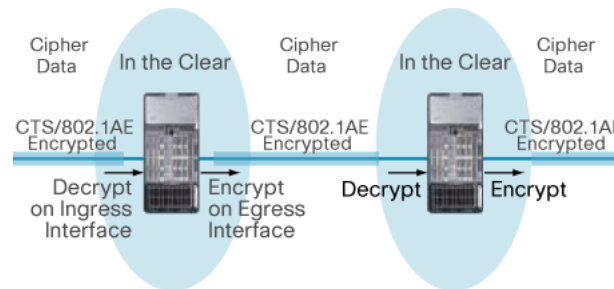
- **アドミッション コントロール**: Cisco Nexus 7000 シリーズは、Authentication, Authorization, and Accounting (AAA; 認証、許可、およびアカウンティング) サーバまたは RADIUS サーバと通信するための組み込み機能を備えています。また、ネットワーク デバイスおよびエンドポイント (有線、無線、およびリモート アクセス) を認証および許可するための、さまざまなプロトコルを使用した包括的な統合ポリシーを提供します。
- **Network Device Admission Control (NDAC; ネットワーク デバイス アドミッション コントロール)**: ネットワーク デバイスはネットワークによって認証される必要があります。
- **Endpoint Admission Control (EAC; エンドポイント アドミッション コントロール)**: アクセス デバイスを認証し、許可ポリシーがユーザまたはデバイス ポートにダウンロードされます。

図 1 企業における Cisco TrustSec



- **LinkSec (IEEE 802.1AE)** : すべてのポートでワイヤレートのリンク層での暗号化が提供されます。パケットは、出力時に暗号化され、入力時に復号化されるので、デバイス内ではクリアテキストの状態になります。この方法により、暗号化されていないトラフィックに対して動作するネットワークサービスを挿入することが可能になり、同時に、ワイヤを通過するトラフィックの完全性とプライバシーが保証されます (図 2 を参照)。

図 2 パケットの機密性と完全性 (IEEE 802.1AE)



システム内で暗号化されないパケット

- **Security Group ACL (SGACL; セキュリティグループ ACL)** : スケーラブルで、トポロジに依存しないこのアクセスコントロールメカニズムは、従来の ACL とは異なります。SGACL グループ ユーザは、特定の Security Group Tag (SGT; セキュリティグループタグ) を使用することで、ACL と同様の権限を持ちます。ポリシーは IP アドレスではなく SGT に基づいているので、ユーザおよびリソースは、セキュリティポリシーを保ったまま、モビリティ (移動の自由) を得ることができます。

認証および許可

Cisco Nexus 7000 シリーズは、不正ユーザからデータセンターを保護するため、IEEE 802.1x や MAC-Auth-Bypass (MAB; MAC 認証バイパス) などのさまざまな認証メカニズムをサポートしています。許可機能は、ACL、VLAN 割り当て、または Cisco TrustSec ポリシーを通じて適用されます。認証および許可情報の伝達には、IEEE 802.1x と共に RADIUS が使用されます。MAB により MAC アドレスベースの認証が可能になり、IEEE 802.1x によりクレデンシャルベースのアイデンティティ検証が可能になります。

Cisco Nexus 7000 シリーズスイッチには、実際の運用でさまざまなレベルの管理アクセス権を付与できます。RBAC では、管理コンソールに対してさまざまなレベルのアクセス権を定義して、適用できます。

統合型セキュリティ機能

Cisco Nexus 7000 シリーズは、Cisco NX-OS 4.0 で実装されている統合型セキュリティと呼ばれるソリューションを利用して、Denial-of-Service (DoS; サービス拒絶) 攻撃、man-in-the-middle 攻撃、不正な DHCP サーバなどからデータセンターネットワークを保護します。

- **Control Plane Policing (CoPP; コントロール プレーン ポリシング)** : Cisco Nexus 7000 シリーズに組み込まれているこのハードウェアベースの機能は、DoS 攻撃からスーパーバイザを保護して、業務に影響を及ぼすサービス停止を阻止します。この機能は、マルチキャストトラフィックをサポートし、Address Resolution Protocol (ARP; アドレス解決プロトコル) およびレイヤ 2 ブロードキャスト ストームや CPU へのトラフィック リダイレクションを阻止するように強化されています。
- **Unicast Reverse Path Forwarding (URPF; ユニキャスト リバース パス転送)** : スプーフされた IP アドレスを持つトラフィックへのアクセスを禁止してネットワークを保護し、正しい送信元ネットワークへのトラフィックの追跡可能性を保証します。Cisco Nexus 7000 シリーズには、同一送信元ネットワークの最大 16 のパスに対してマルチパス URPF チェックを実行するハードウェア機能が組み込まれています。
- **パケットのブロードキャスト抑制** : 帯域幅の可用性にとってリスクのあるポート レベルでのブロードキャスト ストームを阻止して、データ センターのネットワーク パフォーマンスを向上させます。
- **DHCP スヌーピング** : Cisco NX-OS では、信頼できない送信元から受信した DHCP メッセージを検証し、不正なものはフィルタによって除外します。これにより、ポートのセキュリティ保護、MAC アドレスの検証、および IP アドレス割り当ての制限が行われます。
- **IP ソース ガード** : Cisco Nexus 7000 シリーズ ハードウェアによってサポートされ、送信元 IP アドレスをフィルタリングし、悪質なホストによるなりすましを阻止します。

- **Dynamic ARP Inspection (DAI; ダイナミック ARP インспекション)** : ARP スプーフイング (man-in-the-middle 攻撃) および ARP キャッシュ ポイズニングを阻止するため、Cisco NX-OS 4.0 では DAI を使用して ARP パケット内の IP-MAC アドレス バインディングを検証し、合格できなかったパケットをログに記録して破棄します。
- **ポート セキュリティ** : Content-Addressable-Memory (CAM; 連想メモリ) テーブルに対する攻撃 (フラッディング、MAC アドレス スプーフイングなど) を阻止するため、Cisco NX-OS 4.0 では、ポート セキュリティをサポートしてポート入カトラフィックを制限します。

コントロール プレーン保護の拡張

Control Plane Policing (CoPP; コントロール プレーン ポリシング) : このハードウェア ベースの包括的な機能は、DoS 攻撃からスーパーバイザを保護し、ビジネスが中断することがないようにします。Cisco Nexus 7000 シリーズでは、CoPP を拡張して、レイヤ 2 ブロードキャスト ストームを防ぎ、これらのトラフィックが CPU に影響を与えないようにします。

アクセス コントロール リストの拡張

Cisco NX-OS 4.0 は RAACL、VACL、PAACL をサポートし、レイヤ 2、3、4 の各ヘッダー フィールドの照合による Policy Based Routing (PBR; ポリシーベース ルーティング) もサポートします。PBR では、ルーティング メトリックの代わりに管理ポリシーに基づいてパケットをネクスト ホップに転送できるので、データ センター全体の柔軟性とロード シェアリングが向上します。Cisco Nexus 7000 シリーズ ハードウェアは、新しい独自のプログラミング パラダイムである Atomic ACL をサポートしています。この Atomic ACL により、トラフィックを中断することなく ACL を構成できます。Cisco NX-OS 4.0 は、セキュリティ ACL および QoS (Quality Of

Service) ポリシー用に、テスト構成セッションをサポートします。このセッションでユーザは、使用可能なシステム リソースに対する設定を検証してから、それらを採用できます。この選択的なプログラミングによって、データ センターでのスケーラビリティ、使い勝手、およびより優れた管理性も促進されます。

データ センターのセキュリティに投資する理由

Cisco Nexus 7000 スイッチを使用すれば、データ センター内でのセキュリティ展開が容易になり、運用コストが削減されます。

- ロールベース アクセス コントロールによるコストと複雑さの軽減
- 堅牢なコントロールプレーンによる包括的なセキュリティ
- パケットおよびアドレス検証のための複数の統合機能による、パケットの機密性と完全性の確保

関連情報

- Cisco Nexus 7000 シリーズ
www.cisco.com/jp/go/nexus/
- Cisco NX-OS
www.cisco.com/jp/go/nxos/

© 2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。