概要

この章は、Cisco N9300 シリーズ スマート スイッチを紹介します。

はじめに

Cisco N9300 シリーズ スマート スイッチは、高度なネットワーキングおよびセキュリティ機能と、ハードウェア アクセラレーションおよびソフトウェアの柔軟性を組み合わせることで、スケーラブルで安全かつ効率的なデータ センター運用のための統合ソリューションを提供します。

Cisco N9300 シリーズ スマートスイッチは、Hypershield で強化された組み込みセキュリティを提供します。これらのスイッチはサービスを向上させたパフォーマンスを提供し、ネットワークに統合することでセキュリティを簡素化し、個別のファイアウォール構造の必要性を排除します。

Cisco N93000 シリーズ スマート スイッチは、インターコネクトとCloud にまたがって、データセンター内のセキュリティ ゾーンを安全にセグメント化して接続します。

Cisco N9300 シリーズ スマート スイッチ

Cisco N9300 シリーズ スマート スイッチは、データ センター ネットワーキングとセキュリティの機能を拡張するためにデータ処理ユニット（DPU）とネットワーキング ASIC を一緒に統合します。Hypershield は DPU を管理してセキュリティ機能を提供し、NPU は N9000 のルーティングとスイッチングの機能を提供します。

Cisco NX-OS および Hypershield ソフトウェアを単一のソフトウェア イメージに統合することで、デプロイメントが簡素化され、運用の柔軟性が向上します。

Cisco N9300 シリーズ スマート スイッチは、コンバージド スイッチング、ルーティング、レイヤ 4 - レイヤ 7 サービスを提供し、次の機能を備えたレイヤ 2 - レイヤ 7 サービス用のプログラム可能なソフトウェア定義のパイプラインを備えています：

- ハードウェア拡張レイヤ 4 - 7 サービス
- 数百万の接続に対応する拡張できるステートフル ファイアウォール
- ネットワーク サービスの集中制御
- 接続状態の管理
- サービスのインストルメンテーションと分析

Cisco N9324C-SE1U スイッチ

Cisco N9324C-SE1U スイッチは、高性能なネットワーキング機能を提供するように設計された 1 RU ソリューションです。これには、次のような特長があります。

- 24 ポート 100G ポート
- 高速接続と拡張性を提供する Cisco Silicon One E100 ASIC
- ソフトウェア定義型 ステートフル サービス を提供する 4 つの DPU
- 分散レイヤ 4 セグメンテーションや DoS 保護などのサービス

Cisco N9324C-SE1U スイッチのポート スピード

Cisco N9324C-SE1U は、40G および 100G のネイティブ ポート速度をサポートしています。

Cisco N9324C-SE1U は、 でのブレークアウトをサポートしています。

- 4x25G
- 4x10G
- 2x50G

Cisco N9324C-SE1U は、ポートで QSA を使用した 10G をサポートします。

光モジュールのサポート

Cisco N9324C-SE1U はこれらの光ファイバをサポートしています。

- 100G オプティクス
  - QSFP28-100G-SR4
  - QSFP28-100G-PSM4

- QSFP28-100G-CWDM4
- QSFP28-100G-LR4
- QSFP28 AOC、1、3、5、7、10、15、30m
- QSFP28：100G DR、100G FR

- 40G オプティクス
  - QSFP-40G-LR4
  - QSFP AOC、1、3、5、7、10、15、30m
  - QSFP-40G-LR4-S
  - QSFP-40G-SR-BD
  - QSFP-40G-SR4-S
  - QSFP-40G-SR4

サービスイーサネット ポート

サービス イーサネット ポートは、NPU から DPU に トラフィックを伝送するために DPU に割り当てられる一意のタイプのNXOSイーサネットインターフェイスです。これらのポートは、他の既存のインターフェイスタイプと明確に区別するために、帯域内または前面パネルのインターフェイスとは区別されます。

サービスイーサネット ポートは、前面パネルポートと同様に、 MTU、速度、帯域幅などの基本的なインターフェイス設定のデフォルト値を使用して作成されます。service-ethernet ポートは、常に、管理上 UP の状態です。

サービスイーサネット ポートは、DPU がオンラインになり、検出された場合にのみ動作します。DPU がオフラインになるか、サービス アクセラレーション機能が未設定の場合、リンクがダウンする可能性があり、DPU に対応するポートが影響を受けます。

（注） これらのポートは、ISSU のアップグレードを含め、デバイスが再起動されるたびにDPUエージェントによって構成されます。

インターフェイスのステータスを表示するには、 **show interface service-ethernet** *slot/port* コマンドを使用します。

```
Switch# show interface service-ethernet 1/1
admin state is up, Connected to DPU-1
```

show interface hardware-mappings を使用して、DPU からインターフェイスへのマッピングを表示します。

```
Switch# show interface hardware-mappings
```

```
:
--------------------------------------------------------------------------------
Name       Ifindex  Smod Unit HPort NPort Slice Ifg   VPort Serdes_id  service
--------------------------------------------------------------------------------
Eth1/1     1a000000 1    0    16    0     0     0     -1    12
Eth1/2     1a000200 1    0    20    4     0     0     -1    16
Eth1/3     1a000400 1    0    24    8     0     0     -1    20
:
SEth1/1    65000000 1    0    24    8     0     0     -1    20          DPU/1
SEth1/2    65002000 1    0    24    8     0     0     -1    20          DPU/1
SEth1/3    65004000 1    0    24    8     0     0     -1    20          DPU/2
SEth1/4    65006000 1    0    24    8     0     0     -1    20          DPU/2
```

Cisco NX OS および Security Cloud Control

Cisco NX OSコマンド ライン インターフェイス（CLI）およびSecurity Cloud Control を使用して、Cisco N9300 シリーズ スマートスイッチ上の操作を管理できます。

次の表に、Cisco NX OS CLI と Security Cloud Control の操作を示します。

Cisco NX OS CLI	Security Cloud Control
DPUでのトラフィック リダイレクションの管理	セキュリティ ポリシーのライフサイクルの管理と監視
ネットワーク ポリシーの構成	セキュリティポリシーの使用をオーケストレート
ネットワーク分析、トポロジの観測	セキュリティ ポリシーを観測し、セキュリティ コンプライアンスを確保
接続の問題を解決とアシュアランスの提供	スマート スイッチでの Hypershield Agent のアップグレードとダウングレード

Hypershield

Cisco Hypershieldは、最新のデータセンターとクラウド環境を保護するように設計されたAIネイティブの Security Cloud ベースのコントローラ アプリケーションです。Hypershield は、堅牢なセキュリティプロトコルを実装することにより、不正アクセスや潜在的な脅威から保護するためのセキュリティ対策を強化します。

Hypershield は AI によってゼロから構築されており、大量のセキュリティ データの分析、インサイトの生成、インテリジェントな推奨を可能にします。そのハイパー分散型の適用により、セキュリティ メカニズムがサーバーおよびネットワーク インフラストラクチャに統合され、さまざまな場所や環境で保護が提供されます。Hypershield は、すべての適用ポイントでポリシーを一元的に管理および配布し、ネットワーク全体で一貫したセキュリティを確保します。そのカーネル レベルの適用により、オペレーティング システム レベルでの優れた可視性と制御が可能になり、きめ細かいセキュリティアクションが可能になります。その分散型エクスプ

ロイト保護により、新しい脆弱性の補完コントロールを迅速に特定して展開することができ、数分以内に保護を提供します。

Hypershield は次のアセットを管理します。

- **Tesseract Security Agent**： これは、データセンター内で Linux を実行している任意のサーバにインストールされるエージェントであり、セキュリティポリシーの適用を実行する機能を提供します。エージェントは、ネットワーク接続、ファイルおよびシステム コール、ならびにカーネル機能をモニターします。セキュリティイベントを監視および分析するためのイベントベースのテレメトリを生成する。また、NXOS およびサーバー上のセキュリティ イベントまたは PSIRT の AI 自動補完制御を追加することもできます。
- **[ネットワークベースのエンフォーサ（Network-Based Enforcer）]**：トラフィックの転送中に通信フィルタリングを実装するデバイスです。スマート スイッチはネットワーク エンフォーサです。ネットワーク エンフォーサを使用すると、VRF や VLAN などのネットワーク セグメントを保護するレイヤ 3 およびレイヤ 4 ポリシーを作成できます。

Cisco N9300 スマート スイッチは、ネットワーク全体でセキュリティ ポリシーを実装および管理するためのネットワークベースのエンフォーサとして機能します。Cisco N9300 スマート スイッチは、Hypershield のネットワークベースのエンフォーサの下にある Security Cloud Control に表示できます。

N9324C-SE1U スイッチの動作方法

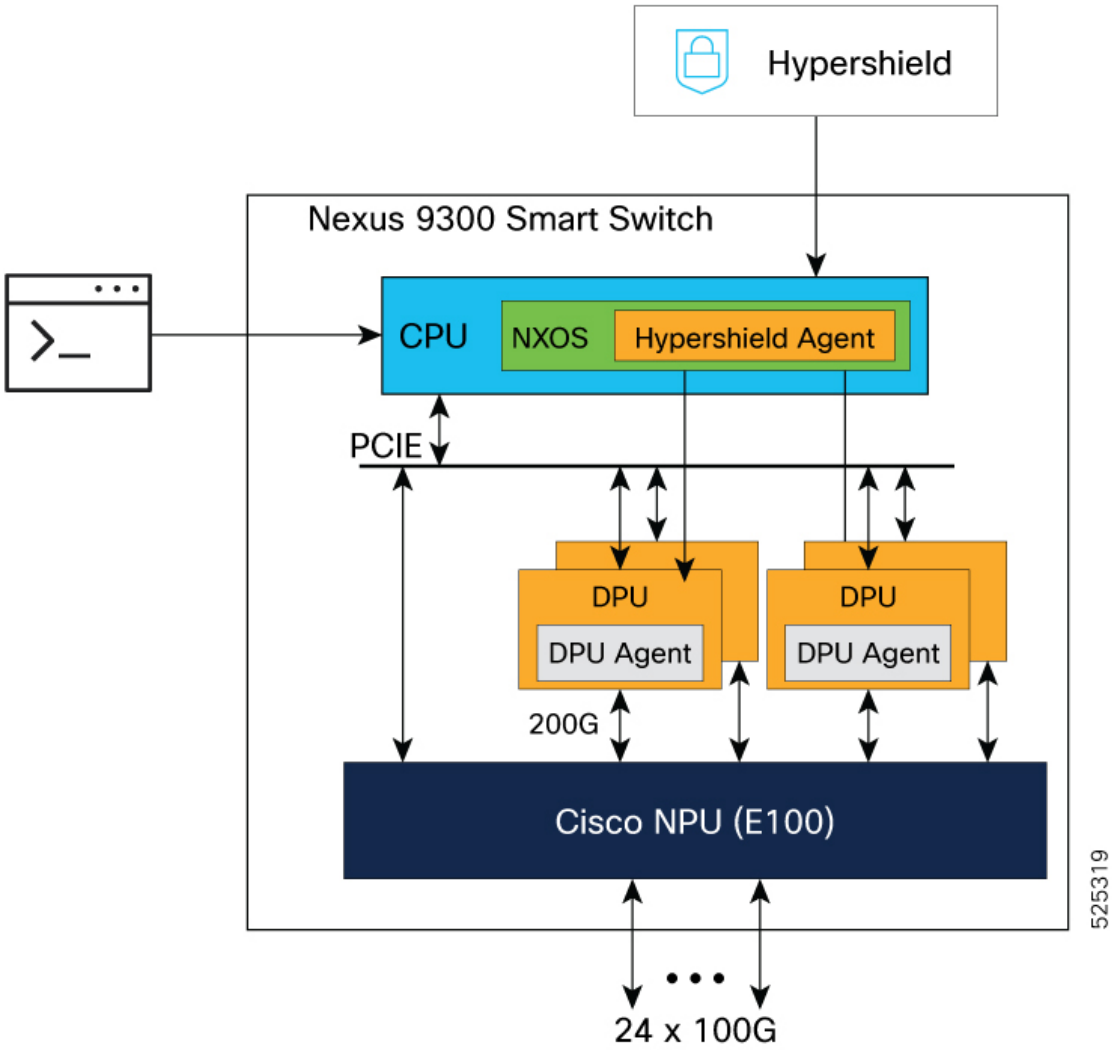
process_summary

Cisco N9324C-SE1U スイッチ アーキテクチャは、ネットワーク トラフィックを管理および処理するためにいくつかの主要コンポーネントを統合しています。コアは、ルーティングとスイッチングを実行する網処理ユニット（NPU）と、通信フィルタリングを実行するデータ処理ユニット（DPU）です。CPU は NXOS オペレーティング システムを実行し、外部 Hyper Shield システムに接続する Hypershield Agent をホストします。ネットワーク構成の管理は、NXOS CLI を介して実行されます。セキュリティ ポリシーの設定は、Hypershield から実行されます。

Cisco N9300 スマートスイッチの Hypershield Agent は、前面パネルポートを介して Hypershield システムへの接続を確立し、送信元インターフェイスのループバック インターフェイスの IP アドレスを使用します。

process_workflow

図 *1 : Cisco N9300* スマート スイッチの動作



これらは、Cisco N9300 スマート スイッチのステージの動作について説明しています。

1. セキュリティ管理者が Hypershield システムでセキュリティ ポリシーを構成すると、これは Cisco N9300 スマート スイッチの Hypershield エージェントにプッシュされます。Hypershield Agent は DPU でそれをプログラムします。
2. Cisco NPU は、他の NXOS デバイスと同様にルーティングとスイッチングを実行します。複数の DPU への 200G リンクで接続されており（Cisco N9324C-SE1U は 4 つの DPU をサポートしています）、構成時に、Cisco NPU はトラフィック検査のためにトラフィックを DPU にリダイレクトすることもできます。

このアーキテクチャにより、DPUは通信フィルタリングのデータプレーン処理を高速化できます。

ソフトウェア管理

NXOS は、Cisco NXOS オペレーティング システムと DPU の両方のソフトウェア イメージを管理します。

- NXOS コンポーネントと Hypershield 管理ソフトウェアの両方をバンドルした特定の NXOS イメージがリリースされています。このようなイメージ名の形式は、`nxos64-s1-dpu.10.5.3s.F.bin`のようなパターンに従います。

Hypershield エージェントの更新は、Hypershield を介して行うことができます。

サポート対象ソフトウェア機能

Cisco Nexus NX- OS リリース 10.5（3s）F では、Cisco N9324C-SE1U および、DPU が有効になっている次のソフトウェア機能のサポートが導入されています。

- マルチ VRF サポートを使用したレイヤ 3 IPv4/IPv6 転送
- VRF ベースのリダイレクション
- ユニキャスト IPv4 および IPv6 ルーテッド トラフィック、ルーテッド ポート、サブインターフェイス、ルーテッド ポート チャネル、およびポート チャネル サブインターフェイスの DPU ベースのトラフィック インスペクション
- BGP、IS-IS、OSPF、EIGRP および static などのルーティング プロトコル
- DPU ライフサイクル管理（ソフトウェア アップグレード、および DPU ヘルス モニタリング）

その他の関連資料

表 *1* : 関連資料

詳細については...	次を参照してください...
Cisco Nexus 9000 シリーズ スイッチ	https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html
Hypershield	https://www.cisco.com/c/en/us/products/collateral/security/hypershield/hypershield-so.html

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。