IPSecの転送中暗号化の設定

ONTAP 9

NetApp
February 12, 2026

目次

IPSecの転送中暗号化の設定

ONTAPネットワークでIPセキュリティを使用するための準備

ONTAP 9.8以降では、必要に応じてIPセキュリティ（IPsec）を使用してネットワーク トラフィックを保護できます。IPSecは、ONTAPで使用できるいくつかの移動中 / 転送中データ暗号化オプションの1つです。本番環境でIPSecを使用する前に、IPSecを設定する準備をしておく必要があります。

ONTAPでのIPセキュリティの実装

IPsecは、IETFによって管理されるインターネット標準です。ネットワーク エンドポイント間を流れるトラフィックの、IPレベルでのデータ暗号化、データ整合性、認証を実現します。

ONTAPでは、ONTAPとさまざまなクライアントの間のあらゆるIPトラフィック（NFS、SMB、iSCSIプロトコルなど）が、IPsecによって保護されます。プライバシーとデータ整合性を確保するだけでなく、リプレイ攻撃や中間者攻撃などの各種攻撃からネットワーク トラフィックを守ります。ONTAPでは、トランスポート モードのIPsec実装を使用します。IPv4かIPv6を使用してONTAPとクライアントの間でキー マテリアルをネゴシエートするために、Internet Key Exchange（IKE）プロトコル バージョン2を利用します。

クラスタでIPSec機能を有効にすると、さまざまなトラフィック特性に一致するONTAPセキュリティ ポリシー データベース（SPD）のエントリが、ネットワークに1つ以上必要になります。これらのエントリは、データの処理と送信に必要な特定の保護の詳細（暗号スイートや認証方式など）にマッピングされます。各クライアントにも、対応するSPDエントリが必要です。

トラフィックの種類によっては、別の移動中データ暗号化オプションが望ましいものもあります。たとえば、NetApp SnapMirrorとクラスタ ピアリング トラフィックの暗号化については、IPsecではなくTransport Layer Security（TLS）プロトコルが一般的に推奨されます。これは、ほとんどの状況でTLSの方が高いパフォーマンスが得られるためです。

関連情報

- "Internet Engineering Task Force"
- "RFC 4301：インターネット プロトコルのセキュリティ アーキテクチャ"

ONTAP IPsec実装の進化

IPsecはONTAP 9.8で初めて導入されました。その実装は、以下に説明するように、その後のONTAPリリースで進化を続けています。

ONTAP 9.18.1

IPsec ハードウェア オフロードのサポートが IPv6 トラフィックに拡張されました。

ONTAP 9.17.1

IPsec ハードウェア オフロードのサポートが"リンク アグリゲーション グループ"に拡張されました。"耐量子事前共有鍵（PPK）"は IPsec 事前共有キー（PSK）認証でサポートされています。

ONTAP 9.16.1

暗号化や整合性チェックなどの暗号化操作の一部は、サポートされているNICカードにオフロードできます。

詳細については、IPSecのハードウェア オフロード機能を参照してください。

ONTAP 9.12.1

MetroCluster IP構成とファブリック接続MetroCluster構成で、フロントエンドのホスト プロトコルとしてIPsecがサポートされました。MetroClusterクラスタでのIPsecのサポートはフロントエンドのホスト トラフィックに限定され、MetroClusterのクラスタ間LIFではサポートされません。

ONTAP 9.10.1

IPsec認証には、PSKに加えて証明書も使用できます。ONTAP 9.10.1より前のバージョンでは、認証にはPSKのみがサポートされています。

ONTAP 9.9.1

IPsecで使用される暗号化アルゴリズムが、FIPS 140-2準拠になりました。これらのアルゴリズムは、FIPS 140-2認定を受けたONTAPのNetApp Cryptographic Moduleで処理されています。

ONTAP 9.8

IPsecのサポートが、トランスポート モードの実装に基づいて初めて利用可能になりました。

IPSecのハードウェア オフロード機能

ONTAP 9.16.1以降を使用している場合、暗号化や整合性チェックなど、計算負荷の高い特定の処理を、ストレージ ノードにインストールされたネットワーク インターフェイス コントローラー（NIC）カードにオフロードするオプションがあります。NICカードにオフロードされた処理のスループットは約5%以下です。これにより、IPsecで保護されたネットワーク トラフィックのパフォーマンスとスループットが大幅に向上します。

要件と推奨事項

IPsecのハードウェア オフロード機能を使用する前に、考慮しておくべき要件がいくつかあります。

サポートされるイーサネット カード

サポートされているイーサネット カードのみをインストールして使用する必要があります。ONTAP 9.16.1 以降では、次のイーサネット カードがサポートされています：

- X50131A（2p、40G/100G/200G/400G Ethernetコントローラ）
- X60132A（4p、10G/25G Ethernet Controller）

ONTAP 9.17.1 では、次のイーサネット カードのサポートが追加されました。

- X50135A（2p、40G/100G Ethernet Controller）
- X60135A（2p、40G/100G Ethernet Controller）

X50131A および X50135A カードは、次のプラットフォームでサポートされています：

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K用
- AFF A90

- AFF A70

X60132A および X60135A カードは、次のプラットフォームでサポートされています：

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20用

サポートされているプラットフォームとカードの詳細については、"NetApp Hardware Universe"を参照してください。

クラスタ スコープ

IPsecハードウェアオフロード機能はクラスタ全体でグローバルに設定されます。そのため、例えば `security ipsec config`コマンドはクラスタ内のすべてのノードに適用されます。

構成の一貫性

サポートされているNICカードが、クラスタ内のすべてのノードに取り付けられている必要があります。サポートされているNICカードが一部のノードでしか使用できない場合、一部のLIFがオフロード対応のNICにホストされていないと、フェイルオーバー後にパフォーマンスが大幅に低下することがあります。

アンチリプレイの無効化

ONTAP（デフォルト設定）およびIPsecクライアントでIPsecアンチリプレイ保護を無効にする必要があります。無効にしない場合、フラグメンテーションとマルチパス（冗長ルート）はサポートされません。

ONTAP IPsec 設定がデフォルトから変更され、アンチリプレイ保護が有効になっている場合は、次のコマンドを使用して無効にします：

```
security ipsec config modify -replay-window 0
```

クライアントでIPsecアンチリプレイ保護が無効になっていることを確認する必要があります。アンチリプレイ保護を無効にするには、クライアントのIPsecドキュメントを参照してください。

制限事項

IPsecのハードウェア オフロード機能を使用する前に、考慮しておくべき制限事項がいくつかあります。

IPv6

ONTAP 9.18.1以降では、IPsecハードウェアオフロード機能でIPv6がサポートされます。ONTAP 9.18.1より前のバージョンでは、IPsecハードウェアオフロードはIPv6をサポートしていません。

拡張シーケンス番号

IPSecの拡張シーケンス番号は、ハードウェア オフロード機能ではサポートされていません。通常の32ビットシーケンス番号のみが使用されます。

リンク アグリゲーション

ONTAP 9.17.1 以降では、IPsec ハードウェア オフロード機能を"リンク アグリゲーション グループ"で使用できます。

9.17.1より前のバージョンでは、IPsecハードウェアオフロード機能はリンクアグリゲーションをサポートしていません。ONTAP CLIの `network port ifgrp`コマンドで管理されるインターフェースまたはリンクアグリゲーショングループでは使用できません。

ONTAP CLIでの設定のサポート

ONTAP 9.16.1では、既存の3つのCLIコマンドが更新され、以下に説明するIPsecハードウェアオフロード機能がサポートされます。詳細については、"ONTAPでのIPセキュリティの設定"も参照してください。

ONTAPコマンド	更新
`security ipsec config show`	ブール型パラメータ `Offload Enabled`は、現在の NIC オフロード ステータスを表示します。
`security ipsec config modify`	このパラメータ `is-offload-enabled`を使用して、NIC オフロード機能を有効または無効にすることができます。
`security ipsec config show-ipsecsa`	インバウンド トラフィックとアウトバウンド トラフィックをバイト数とパケット数で表示するために、4つの新しいカウンタが追加されています。

ONTAP REST APIでの設定のサポート

ONTAP 9.16.1では、以下に説明するように、IPSecのハードウェア オフロード機能をサポートするために、既存の2つのREST APIエンドポイントが更新されています。

RESTエンドポイント	更新
`/api/security/ipsec`	パラメータ `offload_enabled`が追加され、PATCHメソッドで使用できるようになりました。
`/api/security/ipsec/security_association`	オフロード機能で処理された総バイト数とパケット数を追跡するために、2つの新しいカウンタ値が追加されています。

ONTAP REST APIの詳細（ "ONTAP REST APIの新機能"を含む）については、ONTAP自動化ドキュメントを参照してください。 "IPsecエンドポイント"の詳細については、ONTAP自動化ドキュメントも参照してください。

関連情報

- "セキュリティ IPsec"

ONTAPネットワークのIPセキュリティを構成する

ONTAPクラスタでIPSecの転送中暗号化を設定してアクティブ化するためには、いくつかのタスクを実行する必要があります。

IPsec を設定する前に、必ず"IPセキュリティを使用する準備"を確認してください。たとえば、ONTAP 9.16.1以降で使用可能なIPsecハードウェア オフロード機能を使用するかどうかを決定する必要がある場合があります。

クラスタでの**IPsec**の有効化

IPsecをクラスタで有効にすることで、転送中もデータの安全性と暗号化を維持できます。

手順

1. IPsecがすでに有効になっているかどうかを確認します。

   ```
   security ipsec config show
   ```

   結果に `IPsec Enabled: false`が含まれる場合は、次の手順に進みます。

2. IPsecを有効にします。

   ```
   security ipsec config modify -is-enabled true
   ```

   ブール型パラメータ `is-offload-enabled`を使用して、IPsec ハードウェア オフロード機能を有効にできます。

3. 検出コマンドをもう一度実行します。

   ```
   security ipsec config show
   ```

   結果には `IPsec Enabled: true`が含まれるようになりました。

証明書認証用の**IPsec**ポリシーの作成準備

この手順は、認証に事前共有キー（PSK）のみを使用しており、証明書認証を使用しない場合は省略できます。

認証に証明書を使用するIPsecポリシーを作成する前に、次の前提条件を満たしていることを確認する必要があります。

- ONTAPとクライアントの両方がエンド エンティティ（ONTAPまたはクライアント）の証明書を検証できるように、両方に相手側のCA証明書がインストールされている。
- ポリシーの対象になるONTAP LIFの証明書がインストールされている。

> ⓘ 証明書はONTAP LIF間で共有できます。証明書とLIFが1対1で対応している必要はありません。

手順

1. すでにインストールされている場合（ONTAPの自己署名ルートCAの場合）を除き、相互認証で使用するすべてのCA証明書（ONTAP側とクライアント側の両方のCAを含む）をONTAP証明書管理にインストールします。

   サンプル コマンド

   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. 認証中にインストールされている CA が IPsec CA 検索パス内にあることを確認するには、 `security ipsec ca-certificate add`コマンドを使用して ONTAP 証明書管理 CA を IPsec モジュールに追加します。

サンプル コマンド

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
my_ca_cert
```

3. ONTAP LIFで使用する証明書を作成してインストールします。この証明書の発行元CAがすでにONTAPにインストールされ、IPsecに追加されている必要があります。

   サンプル コマンド

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

ONTAPの証明書の詳細については、ONTAP 9のドキュメントのsecurity certificateコマンドを参照してください。

セキュリティ ポリシー データベース（SPD）の定義

IPsecでトラフィックをネットワーク上で転送するためにはSPDエントリが必要です。これは、認証にPSKと証明書のどちらを使用する場合にも当てはまります。

手順

1. `security ipsec policy create`コマンドを使用して次の操作を実行します：
   a. IPsec転送に参加するONTAPのIPアドレスまたはIPアドレスのサブネットを選択します。
   b. ONTAPのIPアドレスに接続するクライアントのIPアドレスを選択します。

      クライアントでInternet Key Exchangeバージョン2（IKEv2）と事前共有キー（PSK）がサポートされている必要があります。

   c. 必要に応じて、トラフィックを保護するための上位層プロトコル（UDP、TCP、ICMPなど）、ローカルポート番号、リモートポート番号などの詳細なトラフィックパラメータを選択します。対応するパラメータは、 `protocols`、 `local-ports`、 `remote-ports`です。

      この手順は、ONTAPのIPアドレスとクライアントのIPアドレスの間のすべてのトラフィックを保護する場合は省略します。デフォルトでは、すべてのトラフィックが保護されます。

   d. 希望する認証方法の `auth-method`パラメータとして、PSK または公開鍵インフラストラクチャ（PKI）を入力します。
      i. PSK を入力する場合は、パラメータを含めて、<enter> を押して事前共有キーを入力して検証します。

         ホストとクライアントの両方がstrongSwanを使用し、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、 `local-identity`および`remote-identity`パラメータはオプションです。

      ii. PKIを入力する場合は、 `cert-name`、 `local-identity`、 `remote-identity`パラメータも入力する必要があります。リモート側の証明書IDが不明な場合、または複数のクライアントIDが想定される場合は、特別なID `ANYTHING`を入力してください。

   e. ONTAP 9.17.1以降では、 `ppk-identity`パラメータを使用して、オプションでポスト量子事前共有鍵（PPK）IDを入力できます。PPKは、将来起こりうる量子コンピュータ攻撃に対するセキュリティをさらに強化します。PPK IDを入力すると、PPKシークレットの入力を求められます。PPKはPSK認証

でのみサポートされます。

`security ipsec policy create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-ipsec-policy-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAPとクライアントの両方で一致するIPsecポリシーが設定され、両方に認証クレデンシャル（PSKまたは証明書）がインストールされるまで、クライアントとサーバの間でIPトラフィックを転送することはできません。

IPsec IDの使用

事前共有キー認証方式では、ホストとクライアントの両方でstrongSwanを使用しており、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、ローカルIDとリモートIDは任意です。

PKI/証明書認証方式では、ローカルIDとリモートIDの両方が必須です。これらのIDは、それぞれの証明書内で認証されるIDを指定し、検証プロセスで使用されます。リモートIDが不明な場合、または複数の異なるIDが使用される可能性がある場合は、特別なID `ANYTHING`を使用してください。

タスク概要

ONTAPでは、SPDエントリを変更するかSPDポリシーの作成時にIDを指定します。SPDには、IPアドレスまたは文字列形式のID名を使用できます。

手順

1. 次のコマンドを使用して、既存のSPD ID設定を変更します。

```
security ipsec policy modify
```

コマンド例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsecの複数クライアント設定

IPsecを利用するクライアントの数が少ない場合は、クライアントごとにSPDエントリを1つ使用するだけで十分です。ただし、数百、数千のクライアントがIPsecを利用する必要がある場合は、IPsecの複数クライアン

ト設定を使用することを推奨します。

タスク概要

ONTAPでは、IPsecを有効にした状態で、単一のSVM IPアドレスに複数のクライアントを多数のネットワーク経由で接続できます。そのためには、次のいずれかの方法を使用します。

- サブネット構成

  特定のサブネット（例：192.168.134.0/24）上のすべてのクライアントが単一のSPDポリシーエントリを使用して単一のSVM IPアドレスに接続できるようにするには、 `remote-ip-subnets`をサブネット形式で指定する必要があります。さらに、 `remote-identity`フィールドに正しいクライアント側IDを指定する必要があります。

  > サブネット設定で単一のポリシー エントリを使用する場合、そのサブネット内のIPsecクライアントはIPsec IDと事前共有キー（PSK）を共有します。ただし、これは証明書認証には当てはまりません。証明書を使用する場合は、各クライアントはそれぞれ固有の証明書か共有の証明書のいずれかを認証に使用できます。ONTAPのIPsecは、証明書の有効性をローカルの信頼ストアにインストールされているCAに基づいてチェックします。証明書失効リスト（CRL）のチェックもサポートされています。

- すべてのクライアント構成を許可する

  送信元 IP アドレスに関係なく、すべてのクライアントが SVM IPsec 対応 IP アドレスに接続できるようにするには、 `remote-ip-subnets`フィールドを指定するときに `0.0.0.0/0`ワイルドカードを使用します。

  さらに、正しいクライアント側IDを `remote-identity`フィールドに指定する必要があります。証明書認証の場合は、 `ANYTHING`と入力できます。

  また、 `0.0.0.0/0`ワイルドカードを使用する場合は、使用するローカルまたはリモートのポート番号を具体的に設定する必要があります。例： `NFS port 2049`

  手順

  a. 次のいずれかのコマンドを使用して、複数クライアント向けのIPsecを設定します。

     i. 複数の IPsec クライアントをサポートするために サブネット構成 を使用している場合：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     コマンド例

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. 複数の IPsec クライアントをサポートするために すべてのクライアントを許可する構成 を使用している場合：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

コマンド例

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

IPSecの統計の表示

ネゴシエーションを通じて、ONTAP SVMのIPアドレスとクライアントのIPアドレスの間に、IKEセキュリティ アソシエーション（SA）と呼ばれるセキュリティ チャネルが確立されます。実際のデータの暗号化と復号化を実行するために、両方のエンドポイントにIPsec SAがインストールされます。統計コマンドを使用して、IPsec SAとIKE SAの両方のステータスを確認できます。

IPsec ハードウェア オフロード機能を使用している場合は、コマンド `security ipsec config show-ipsecsa`でいくつかの新しいカウンターが表示されます。

コマンド例

IKE SAのコマンドの例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SAのコマンドと出力の例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SAのコマンドと出力の例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
             Policy  Local           Remote          Inbound  Outbound
Vserver      Name    Address         Address         SPI      SPI
State
------------ ------- --------------- --------------- -------- --------
---------
vs1          test34
                     192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

関連情報

- "security certificate install"
- "セキュリティ IPsec"

著作権に関する情報

商標に関する情報