IPSec転送中暗号化の設定

ONTAP 9

NetApp
December 20, 2024

目次

IPSec転送中暗号化の設定

IPセキュリティを使用する準備

ONTAP 9 .8以降では、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するオプションが用意されています。IPSecは、ONTAPで使用できる複数の転送中データ暗号化または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によって維持されているインターネット標準です。IPレベルでネットワークエンドポイント間を流れるトラフィックに対して、データの暗号化と整合性、および認証を提供します。

ONTAPでは、ONTAPとさまざまなクライアント（NFS、SMB、iSCSIプロトコルを含む）の間のすべてのIPトラフィックがIPsecによって保護されます。プライバシーとデータの整合性に加えて、ネットワークトラフィックはリプレイ攻撃や中間者攻撃などのいくつかの攻撃から保護されます。ONTAPでは、IPsecトランスポートモードの実装が使用されます。Internet Key Exchange（IKE;インターネットキーエクスチェンジ）プロトコルバージョン2を利用して、IPv4またはIPv6を使用してONTAPとクライアント間でキーマテリアルをネゴシエートします。

クラスタでIPSec機能を有効にすると、ネットワークでは、ONTAPセキュリティポリシーデータベース（SPD）にさまざまなトラフィック特性に一致するエントリが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、認証方式など）にマッピングされます。各クライアントには、対応するSPDエントリも必要です。

トラフィックの種類によっては、別の転送中データ暗号化オプションを使用することをお勧めします。たとえば、NetApp SnapMirrorおよびクラスタピアリングトラフィックの暗号化には、一般に、IPsecではなくTransport Layer Security（TLS）プロトコルが推奨されます。これは、ほとんどの状況でTLSの方がパフォーマンスが向上するためです。

関連情報

- "インターネット技術タスクフォース"
- "RFC 4301：『Security Architecture for the Internet Protocol』"

ONTAP IPsec実装の進化

IPsecは最初にONTAP 9で導入されました。8.実装は、次のように進化し、改善され続けています。

特定のONTAPリリース以降に導入された機能は、特に記載がないかぎり、以降のリリースでもサポートされます。

ONTAP 9 .16.1

暗号化や整合性チェックなどの暗号化処理のいくつかは、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、を参照してください IPSecハードウェアオフロード機能 。

ONTAP 9 12.1

IPSecフロントエンド・ホスト・プロトコルは、MetroCluster IPおよびMetroClusterファブリック接続構成で

サポートされます。MetroClusterクラスタで提供されるIPSecのサポートはフロントエンドホストトラフィックに限定され、MetroClusterクラスタ間LIFではサポートされません。

ONTAP 9 10.1

証明書は、事前共有キー（PSK）に加えて、IPsec認証にも使用できます。PSK .10.1より前のONTAP 9バージョンでは、PSKのみが認証でサポートされていました。

ONTAP 9 .9.1

IPsecで使用される暗号化アルゴリズムはFIPS 140-2に準拠しています。これらのアルゴリズムは、ONTAPのNetApp暗号モジュールによって処理され、FIPS 140-2の検証が行われます。

ONTAP 9.8

IPsecのサポートは、最初はトランスポートモードの実装に基づいて利用可能になります。

IPSec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は、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取り付けられたNetwork Interface Controller（NIC;ネットワークインターフェイスコントローラ）カードにオフロードすることができます。このハードウェアオフロードオプションを使用すると、IPsecで保護される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ハードウェアオフロード機能を使用する前に、いくつかの要件を考慮する必要があります。

サポートされるイーサネットカード

ストレージノードに取り付けて使用する必要があるのは、サポートされているイーサネットカードだけです。ONTAP 9 .16.1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イーサネットコントローラ CX7）
- X60243A（4p、10G/25Gイーサネットコントローラ CX7）

クラスタスコープ

IPSecハードウェアオフロード機能は、クラスタに対してグローバルに設定されます。たとえば、コマンドは`security ipsec config`クラスタ内のすべてのノードに適用されます。

一貫した構成

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、オフロードに対応したNICで一部のLIFが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。

アンチリプレイを無効にする

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

制限事項

IPsecハードウェアオフロード機能を使用する前に、いくつかの制限事項を考慮する必要があります。

IPv6

IPバージョン6は、IPsec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。IPv6は、IPsecソフトウェア実装でのみサポートされます。

拡張シーケンス番号

IPSec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

IPSecハードウェアオフロード機能では、リンクアグリゲーションはサポートされません。そのため、ONTAP CLIのコマンドで管理するインターフェイ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 `network port ifgrp`。

ONTAP CLIでの設定のサポート

ONTAP 9 .16.1では、次に説明するように、3つの既存のCLIコマンドが更新され、IPSecハードウェアオフロード機能がサポートされています。詳細については、も参照してください"ONTAPでのIPセキュリティの設定"。

ONTAPコマンド	更新
`security ipsec config show`	ブーリアンパラメータは `Offload Enabled`、現在のNICオフロードステータスを示します。
`security ipsec config modify`	パラメータを `is-offload-enabled`使用して、NICオフロード機能を有効または無効にできます。
`security ipsec config show-ipsecsa`	インバウンドおよびアウトバウンドトラフィックをバイトおよびパケット単位で表示するために、4つの新しいカウンタが追加されました。

ONTAP REST APIでの設定のサポート

ONTAP 9 .16.1では、次に説明するように、2つの既存のREST APIエンドポイントが更新され、IPsecハードウェアオフロード機能がサポートされます。

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ました。

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

ONTAPでのIPセキュリティの設定

ONTAPクラスタで転送中のIPSec暗号化を設定してアクティブにするには、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、を確認してください"IPセキュリティを使用する準備"。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IPSecを有効にする

クラスタでIPSecを有効にすると、転送中もデータが継続的に暗号化されてセキュアになるようにすることができます。

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
   ```

   結果にが含まれている場合は `IPsec Enabled: false`、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
   ```

   IPSecハードウェアオフロード機能は、ブーリアンパラメータを使用してイネーブルにできます `is-offload-enabled`。

3. 検出コマンドを再度実行します。

   ```
   security ipsec config show
   ```

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

証明書認証を使用したIPSecポリシーの作成の準備

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

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. 相互認証で使用したすべてのCA証明書（ONTAP側CAとクライアント側CAの両方を含む）をONTAP証明書管理にインストールします（ONTAPの自己署名ルートCAの場合など）。

   サンプルコマンド
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   ```

```
-cert-name my_ca_cert
```

2. インストールされているCAが認証時にIPsec CA検索パス内にあることを確認するには、コマンドを使用して、IPsecモジュールにONTAP証明書管理CAを追加し `security ipsec ca-certificate add`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。この証明書の発行者CAが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. コマンドを使用し `security ipsec policy create`て次の処理を行います
   a. ONTAP転送に参加する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 IPアドレスに接続するクライアントIPアドレスを選択します。

      クライアントは、事前共有キー（PSK）を使用してInternet Key Exchangeバージョン2（IKEv2）をサポートしている必要があります。

   c. オプション。トラフィックを保護するために、上位レイヤプロトコル（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、きめ細か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`、それぞれ、 `local-ports`および `remote-ports`です。

      ONTAP IPアドレスとクライアントIPアドレス間のすべてのトラフィックを保護するには、この手順を省略します。すべてのトラフィックを保護することがデフォルトです。

   d. 目的の認証方式のパラメータにPSKまたは公開キーインフラストラクチャ（PKI）を入力します `auth-method`。
      i. PSKを入力する場合は、パラメータを指定し、<enter>キーを押して事前共有キーの入力と確認を求めるプロンプトを表示します。

         `local-identity`ホストとクライアントの両方で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、パラメータと `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、、 `local-identity`、 `remote-identity`パラメータも入力する必要があり

`cert-name`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が予想される場合は、特別なIDを入力し `ANYTHING`ます。

```
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が一致するIPsecポリシーを設定し、認証クレデンシャル（PSKまたは証明書）が両側に配置されるまで、IPトラフィックはクライアントとサーバの間を流れません。

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 / 証明書を使用する認証方式では、ローカルとリモートの両方のIDが必須です。IDはONTAPとクライアントそれぞれの証明書でどのIDが認定されているかを示すもので、検証プロセスで使用されます。リモートIDが不明な場合、または多数の異なるIDである可能性がある場合は、特別なIDを使用し `ANYTHING`ます。

タスクの内容

ONTAP内では、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名を指定できます。

手順

1. 既存のSPD ID設定を変更するには、次のコマンドを使用します。

```
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を利用する必要があ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1つのSPDエントリを使用すれば十分です。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、NetApp IPsecの複数クライアント構成を使用することを推奨します。

タスクの内容

ONTAPでは、IPSecを有効にした状態で、1つの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。これには、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（192.168.134.0/24など）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、をサブネット形式で指定する必要があります `remote-ip-subnets`。また、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 `remote-identity`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設定を許可 *

  ソースIPアドレスに関係なくすべてのクライアントがSVMのIPsec対応IPアドレスに接続できるようにするには `0.0.0.0/0`、フィールドにワイルドカードを指定し `remote-ip-subnets`ます。

  また、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 `remote-identity`ます。証明書認証の場合は、と入力できます `ANYTHING`。

  また、ワイルドカードを使用する場合は `0.0.0.0/0`、使用する特定のローカルまたはリモートポート番号を設定する必要があります。たとえば、 `NFS port 2049`です。

  手順

  a. 複数のクライアントに対してIPsecを設定するには、次のいずれかのコマンドを使用します。

     i. サブネット設定*を使用して複数のIPsecクライアントをサポートする場合：

     ```
     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. [すべてのクライアントの設定を許可する]*を使用して複数のIPsecクライアントをサポートする場合は、次の手順を実行します。

     ```
     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統計を表示します。

ネゴシエーションを使用すると、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を確立できます。IPsec SAは、実際のデータ暗号化および復号化作業を行うために、両方のエンドポイントにインストールされます。statistics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、コマンドでいくつかの新しいカウンタが表示され `security ipsec config show-ipsecsa`ます。

コマンド例

IKE SAサンプルコマンド：

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

ipsec saコマンドおよび出力例：

```
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コマンドおよび出力例：

```
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
```

著作権に関する情報

商標に関する情報