



ネットワークのセキュリティを確保 ONTAP 9

NetApp
December 20, 2024

目次

ネットワークのセキュリティを確保	1
連邦情報処理標準（FIPS）を使用したネットワークセキュリティの設定	1
IPSec転送中暗号化の設定	4
LIFのファイアウォールポリシーを設定する	12
ファイアウォールサービスとポリシーの管理用コマンド	18

ネットワークのセキュリティを確保

連邦情報処理標準（FIPS）を使用したネットワークセキュリティの設定

ONTAPは、すべてのSSL接続について、連邦情報処理標準（FIPS）140-2に準拠しています。ONTAPでは、SSL FIPSモードをオンまたはオフにしたり、SSLプロトコルをグローバルに設定したり、RC4などの弱い暗号を無効にしたりできます。

デフォルトでは、次のコマンドを使用して、ONTAPのSSLはFIPS準拠を無効にし、SSLプロトコルを有効にして設定されます。

- TLSv1.3（ONTAP 9.11.1以降）
- TLSv1.2
- TLSv1.1
- TLSv1

SSL FIPSモードが有効な場合、ONTAPからONTAPの外部のクライアントまたはサーバコンポーネントへのSSL通信では、SSL用のFIPS準拠の暗号が使用されます。

管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにする場合は、SSL FIPSモードを有効にする前に、ホストキーのアルゴリズムがサポートされていることを確認する必要があります。

*注：ONTAP 9.11.1以降では、ホストキーアルゴリズムのサポートが変更されています。

ONTAP リリース	サポートされているキータイプ	サポートされていないキータイプです
9.11.1以降	ECDSA - sha2 - nistp256	rsa-sha2-512+ rsa-sha2-256+ ssh-ed25519 + ssh-dss+ssh-rsa
9.10.1以前	ECDSA - sha2 -nistp256 + ssh-ed25519	SSH-DSS + ssh-rsa

FIPSを有効にする前に、サポートされているキーアルゴリズムがない既存のSSH公開鍵アカウントをサポートされているキータイプで再設定する必要があります。そうしないと、管理者認証が失敗します。

詳細については、を参照してください ["SSH公開鍵アカウントの有効化"](#)。

SSL FIPSモードの設定の詳細については、のマニュアルページを参照して `security config modify` ください。

FIPSを有効にする

システムのインストールまたはアップグレードの直後に、すべてのセキュアなユーザがセキュリティ設定を調整することをお勧めします。SSL FIPSモードが有効な場合、ONTAPからONTAPの外部のクライアントまたはサーバコンポーネントへのSSL通信では、SSL用のFIPS準拠の暗号が使用されます。



FIPSが有効な場合、RSAキーの長さが4096の証明書をインストールまたは作成することはできません。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. FIPSを有効にします。

```
security config modify -interface SSL -is-fips-enabled true
```

3. 続行するかどうかを尋ねられたら、 y

4. ONTAP 9 .8以前を実行している場合は、クラスタ内の各ノードを1つずつ手動でリブートします。ONTAP 9.9.1以降では、リブートは必要ありません。

例

ONTAP 9 .9.1以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -interface SSL -is-fips-enabled true
```

```
Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.
```

```
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

FIPSの無効化

古いシステム構成を実行していて、ONTAPを下位互換性のある方法で設定したい場合は、FIPSが無効になっている場合にのみSSLv3を有効にできます。

手順

1. advanced権限レベルに切り替えます。

```
set -privilege advanced
```

2. FIPSを無効にするには、

```
security config modify -interface SSL -is-fips-enabled false
```

3. 続行するかどうかを尋ねられたら、と入力し `y` します。
4. ONTAP 9.8以前を実行している場合は、クラスタ内の各ノードを手動でリブートします。ONTAP 9.9.1以降では、リブートは必要ありません。

例

ONTAP 9.9.1以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -interface SSL -supported-protocols SSLv3
```

```
Warning: Enabling the SSLv3 protocol may reduce the security of the  
interface, and is not recommended.
```

```
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster.  
This is necessary to prevent components from failing due to an  
inconsistent security configuration state in the cluster. To avoid a  
service outage, reboot one node at a time and wait for it to completely  
initialize before rebooting the next node. Run "security config status  
show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

FIPS準拠ステータスの表示

クラスタ全体で現在のセキュリティ設定が実行されているかどうかを確認できます。

手順

1. クラスタ内の各ノードを1つずつリブートします。

すべてのクラスタノードを同時にリブートしないでください。クラスタ内のすべてのアプリケーションで新しいセキュリティ設定が実行されるようにするには、リブートが必要です。また、FIPSのオン/オフモード、プロトコル、および暗号に対するすべての変更を行うには、リブートが必要です。

2. 現在の準拠ステータスを表示します。

```
security config show
```

```
security config show
```

```

                Cluster
Security
Interface FIPS Mode   Supported Protocols   Supported Ciphers Config
Ready
-----
-----
SSL          false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL: yes
                                   !EXP:!eNULL
```

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せん。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
<code>security ipsec config show</code>	ブーリアンパラメータは <code>Offload Enabled</code> 、現在のNICオフロードステータスを示します。
<code>security ipsec config modify</code>	パラメータを <code>'is-offload-enabled'</code> 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。
<code>security ipsec config show-ipsecsa</code>	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
<code>/api/security/ipsec</code>	パラメータ <code>'offload_enabled'</code> が追加され、PATCHメソッドで使用できるようになりました。

RESTエンドポイント	更新
/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` で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ます '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、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ます `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ます `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          Initiator-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

```

LIFのファイアウォールポリシーを設定する

ファイアウォールを設定すると、クラスタのセキュリティが強化され、ストレージシステムへの不正アクセスを防止できます。デフォルトでは、オンボードファイアウォールは、データLIF、管理LIF、およびクラスタ間LIFに対して特定のIPサービスセットへのリモートアクセスを許可するように設定されています。

ONTAP 9.10.1以降：

- ファイアウォールポリシーは廃止され、LIFのサービスポリシーに置き換えられました。以前は、オンボードファイアウォールはファイアウォールポリシーを使用して管理されていました。これにはLIFサービスポリシーを使用します。
- ファイアウォールポリシーはすべて空で、基盤となるファイアウォールのポートは開かれません。代わりに、LIFサービスポリシーを使用してすべてのポートを開く必要があります。
- 9.10.1以降にアップグレードしたあとも、ファイアウォールポリシーからLIFのサービスポリシーに移行するための対処は必要ありません。以前のONTAPリリースで使用していたファイアウォールポリシーと整合性のあるLIFのサービスポリシーが自動的に作成されます。カスタムファイアウォールポリシーを作成および管理するスクリプトやその他のツールを使用する場合は、それらのスクリプトをアップグレードしてカスタムサービスポリシーを作成する必要があります。

詳細については、を参照してください"[ONTAP 9.6以降のLIFとサービスポリシー](#)"。

ファイアウォールポリシーを使用して、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、SNMPなどの管理サービスプロトコルへのアクセスを制御できます。NFSやSMBなどのデータプロトコルにファイアウォールポリシーを設定することはできません。

ファイアウォールサービスとポリシーは次の方法で管理できます。

- ファイアウォールサービスの有効化と無効化
- 現在のファイアウォールサービス設定の表示
- ポリシー名とネットワークサービスを指定して新しいファイアウォールポリシーを作成する
- 論理インターフェイスへのファイアウォールポリシーの適用
- 既存のポリシーとまったく同じ新しいファイアウォールポリシーを作成する

この機能は、同じSVM内で同様の特性を持つポリシーを作成する場合や、別のSVMにポリシーをコピーする場合に使用できます。

- ファイアウォールポリシーに関する情報の表示
- ファイアウォールポリシーで使用されるIPアドレスとネットマスクの変更
- LIFで使用されていないファイアウォールポリシーを削除する

ファイアウォールポリシーとLIF

LIFのファイアウォールポリシーは、各LIFを介したクラスタへのアクセスを制限するために使用されます。デフォルトのファイアウォールポリシーが各タイプのLIFを介したシステムアクセスに与える影響と、ファイアウォールポリシーをカスタマイズしてLIFのセキュリティを増減する方法を理解しておく必要があります。

コマンドまたは `network interface modify` コマンドを使用してLIFを設定する場合、 `network interface create` パラメータに指定した値 `firewall-policy` によって、LIFへのアクセスが許可されるサービスプロトコルとIPアドレスが決まります。

多くの場合、デフォルトのファイアウォールポリシーの値をそのまま使用できます。また、特定のIPアドレスや管理サービスプロトコルへのアクセスを制限しなければならない場合もあります。使用可能な管理サービスプロトコルには、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、およびSNMPがあります。

すべてのクラスタLIFのファイアウォールポリシーはデフォルトで設定されており、変更することはできません。

次の表に、LIFの作成時にロール（ONTAP 9.5以前）またはサービスポリシー（ONTAP 9.6以降）に応じて各LIFに割り当てられるデフォルトのファイアウォールポリシーを示します。

ファイアウォールポリシー	デフォルトのサービスプロトコル	デフォルトのアクセス	適用先のLIF
管理	dns、http、https、ndmp、ndmps、ntp、snmp、ssh	任意のアドレス（0.0.0.0/0）	クラスタ管理 LIF、SVM 管理 LIF、ノード管理 LIF
管理- NFS	dns、http、https、ndmp、ndmps、ntp、portmap、snmp、ssh	任意のアドレス（0.0.0.0/0）	SVM 管理アクセスもサポートするデータ LIF
クラスタ間	HTTPS、NDMP、ndmps	任意のアドレス（0.0.0.0/0）	すべてのクラスタ間LIF
データ	DNS、NDMP、ndmps、portmap	任意のアドレス（0.0.0.0/0）	すべてのデータLIF

portmapサービスの設定

portmapサービスは、RPCサービスをリッスンするポートにマッピングします。

portmapサービスはONTAP 9.3以前では常にアクセス可能であり、ONTAP 9.4ではONTAP 9.6を使用して設定可能になり、ONTAP 9.7から自動的に管理されるようになりました。

- ONTAP 9.3以前では、サードパーティ製のファイアウォールではなく組み込みのONTAPファイアウォールを使用するネットワーク構成では、ポート111でportmapサービス（rpcbind）に常にアクセスできました。
- ONTAP 9.4~lif.6 ONTAP 9では、ファイアウォールポリシーを変更して、portmapサービスへのアクセスを許可するかどうかをLIFごとに制御できます。
- ONTAP 9.7以降では、portmapファイアウォールサービスは廃止されています。代わりに、NFSサービスをサポートするすべてのLIFに対してportmapポートが自動的に開きます。
- ポートマップサービスは、ONTAP 9.4 ~ ONTAP 9.6* のファイアウォールで設定可能です

このトピックの残りの部分では、ONTAP 9.4~ONTAP 9.6リリースのportmapファイアウォールサービスを設定する方法について説明します。

構成によっては、特定のタイプのLIF（通常は管理LIFとクラスタ間LIF）でサービスへのアクセスを禁止することができます。状況によっては、データLIFへのアクセスを禁止することもできます。

想定される動作

ONTAP 9.4~ONTAP 9.6の動作は、アップグレード時にシームレスに移行できるように設計されています。portmapサービスにすでに特定のタイプのLIFからアクセスしている場合、それらのタイプのLIFからは引き続きサービスにアクセスできます。ONTAP 9.3以前と同様に、ファイアウォール内でアクセスを許可するサービスをLIFのタイプ別のファイアウォールポリシーで指定できます。

この動作を有効にするには、クラスタ内のすべてのノードでONTAP 9.4~ONTAP 9.6が実行されている必要があります。影響するのはインバウンドトラフィックのみです。

新しいルールは次のとおりです。

- リリース9.4~9.6にアップグレードすると、既存のすべてのファイアウォールポリシー（デフォルトまたはカスタム）にportmapサービスが追加されます。
- 新しいクラスタやIPspaceを作成した場合、portmapサービスはデフォルトのデータポリシーにのみ追加され、デフォルトの管理ポリシーまたはクラスタ間ポリシーには追加されません。
- 必要に応じて、デフォルトまたはカスタムのポリシーにportmapサービスを追加したり削除したりできます。

portmapサービスを追加または削除する方法

SVMまたはクラスタのファイアウォールポリシーにportmapサービスを追加する（ファイアウォール内でのアクセスを許可する）には、次のように入力します。

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

SVMまたはクラスタのファイアウォールポリシーからportmapサービスを削除する（ファイアウォール内でのアクセスを禁止する）には、次のように入力します。

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

network interface modifyコマンドを使用して既存のLIFにファイアウォールポリシーを適用できます。コマン

ド構文全体については、を参照してください ["ONTAPコマンド リファレンス"](#)。

ファイアウォールポリシーを作成してLIFに割り当てる

LIFの作成時に、デフォルトのファイアウォールポリシーが各LIFに割り当てられます。多くの場合、ファイアウォールのデフォルト設定をそのまま使用でき、変更する必要はありません。ただし、LIFにアクセスできるネットワーク サービスやIPアドレスを変更したい場合は、カスタム ファイアウォール ポリシーを作成してLIFに割り当てます。

タスクの内容

- `intercluster`、`cluster`、またはの `mgmt`名前`data`` でファイアウォールポリシーを作成することはできません `policy`。

これらの値は、システム定義のファイアウォールポリシー用に予約されています。

- クラスタLIFのファイアウォールポリシーを設定または変更することはできません。

クラスタLIFのファイアウォールポリシーは、すべてのサービスタイプで0.0.0.0/0に設定されます。

- ポリシーからサービスを削除する必要がある場合は、既存のファイアウォールポリシーを削除して新しいポリシーを作成する必要があります。
- クラスタでIPv6が有効になっている場合は、IPv6アドレスを使用してファイアウォールポリシーを作成できます。

IPv6を有効にすると、`data`、`intercluster` および `mgmt`ファイアウォールポリシーの有効なアドレスのリストに::/0というIPv6ワイルドカードが含まれます。`

- System Managerを使用してクラスタ全体のデータ保護機能を設定する場合は、許可されるアドレスのリストにクラスタ間LIFのIPアドレスを含め、クラスタ間LIFと会社所有のファイアウォールの両方でHTTPSサービスを許可する必要があります。

デフォルトでは、ファイアウォールポリシーは `intercluster`すべてのIPアドレス (IPv6の場合は0.0.0.0/0、または::/0) からのアクセスを許可し、HTTPS、NDMP、およびNDMPサービス` を有効にします。このデフォルトポリシーを変更する場合、またはインタークラスタLIF用に独自のファイアウォールポリシーを作成する場合は、許可されるリストに各インタークラスタLIFのIPアドレスを追加し、HTTPSサービスを有効にする必要があります。

- ONTAP 9 .6以降では、HTTPSおよびSSHファイアウォールサービスはサポートされていません。

ONTAP 9 .6では `management-https management-ssh`、HTTPSおよびSSH管理アクセスにLIFサービスとLIFサービスを使用できます。

手順

1. 特定のSVMのLIFで使用できるファイアウォールポリシーを作成します。

```
system services firewall policy create -vserver vserver_name -policy policy_name -service network_service -allow-list ip_address/mask
```

このコマンドを複数回使用して、ファイアウォールポリシーに複数のネットワークサービスと各サービスで許可されるIPアドレスのリストを追加できます。

2. コマンドを使用して、ポリシーが正しく追加されたことを確認します `system services firewall policy show`。

3. ファイアウォールポリシーをLIFに適用します。

```
network interface modify -vserver vserver_name -lif lif_name -firewall-policy policy_name
```

4. コマンドを使用して、ポリシーがLIFに正しく追加されたことを確認します `network interface show -fields firewall-policy`。

ファイアウォールポリシーを作成してLIFに割り当てる例

次のコマンドは、10.10サブネットのIPアドレスからのHTTPおよびHTTPSプロトコルによるアクセスを許可するdata_httpというファイアウォールポリシーを作成し、SVM vs1のdata1というLIFに適用してから、クラスタのすべてのファイアウォールポリシーを表示します。

```
system services firewall policy create -vserver vs1 -policy data_http -service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

Vserver	Policy	Service	Allowed

cluster-1	data		
		dns	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1	intercluster		
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1	mgmt		
		dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
vs1	data_http		
		http	10.10.0.0/16
		https	10.10.0.0/16

```
network interface modify -vserver vs1 -lif data1 -firewall-policy data_http
```

```
network interface show -fields firewall-policy
```

vserver	lif	firewall-policy

Cluster	node1_clus_1	
Cluster	node1_clus_2	
Cluster	node2_clus_1	
Cluster	node2_clus_2	
cluster-1	cluster_mgmt	mgmt
cluster-1	node1_mgmt1	mgmt
cluster-1	node2_mgmt1	mgmt
vs1	data1	data_http
vs3	data2	data

ファイアウォールサービスとポリシーの管理用コマンド

ファイアウォールサービスを管理するにはコマンド、ファイアウォールポリシーを管理する `network interface modify` にはコマンド、`system services firewall policy` LIFのファイアウォール設定を管理するにはコマンドを使用し `system services firewall` ます。

状況	使用するコマンド
ファイアウォールサービスを有効または無効にする	<code>system services firewall modify</code>
ファイアウォールサービスの現在の設定を表示する	<code>system services firewall show</code>
ファイアウォールポリシーを作成するか、既存のファイアウォールポリシーにサービスを追加する	<code>system services firewall policy create</code>
ファイアウォールポリシーをLIFに適用する	<code>network interface modify -lif lifname -firewall-policy</code>
ファイアウォールポリシーに関連付けられているIPアドレスとネットマスクを変更する	<code>system services firewall policy modify</code>
ファイアウォールポリシーに関する情報を表示する	<code>system services firewall policy show</code>
既存のポリシーとまったく同じ新しいファイアウォールポリシーを作成する	<code>system services firewall policy clone</code>
LIFで使用されていないファイアウォールポリシーを削除する	<code>system services firewall policy delete</code>

詳細については `system services firewall policy network interface modify`、の各コマンドのマニュアルページを参照して `system services firewall` "[ONTAP 9コマンドリファレンス](#)" ください。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。