

ネットワークを保護します ONTAP 9

NetApp September 12, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/networking/configure_network_security_using_federal_information_processing_standards_@fips @.html on September 12, 2024. Always check docs.netapp.com for the latest.

目次

ネ	ットワークを保護します	. 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
	ワイヤ暗号化を介した IP セキュリティ(IPsec)を設定します · · · · · · · · · · · · · · · · · · ·	. 4
	LIF のファイアウォールポリシーを設定します	. 9
	ファイアウォールサービスおよびポリシーを管理するためのコマンド・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	15

ネットワークを保護します

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 接続に対する連邦情報処理標準(FIPS) 140-2 に準拠して います。ONTAP では、 SSL FIPS モードを有効または無効にしたり、 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、 ONTAP の SSL は、次のプロトコルを使用して FIPS 準拠が無効、 SSL プロトコルが有効 な状態で設定されます。

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

SSL FIPS モードがイネーブルの場合、 ONTAP から ONTAP 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 通信には、 FIPS 準拠の SSL 用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以降 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、サポートされるキーアルゴリズムを使用していない既存の SSH 公開鍵アカウント をサポート対象のキータイプで再設定する必要があります。再設定しないと、管理者認証は失敗します。

詳細については、を参照してください "SSH 公開鍵アカウントを有効にします"。

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

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、すべてのセキュアユーザがセキュリティ設定を調整 することを推奨します。SSL FIPS モードがイネーブルの場合、 ONTAP から ONTAP 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 通信には、 FIPS 準拠の SSL 用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

- 続行するかどうかを尋ねられたら、と入力します y
- 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 を無効にする

古いシステム構成を実行し続けている状況で、 ONTAP の設定で下位互換性を確保する場合は、 FIPS が無効 な場合にのみ SSLv3 を有効にすることができます。

手順

1. advanced 権限レベルに切り替えます。

set -privilege advanced

2. 次のように入力して FIPS を無効に

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

- 続行するかどうかを尋ねられたら、と入力します 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 準拠ステータスを表示します

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することができます。

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ていること、および FIPS のオン / オフモード、プロトコル、暗号に 対する変更がすべて反映されていることを確認するには、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				
- I.	Cluster			Cluster
Security Interface Ready	FIPS Mode	Supported Protocols	Supported Ciphers	Config
SSL	false	TLSv1_2, TLSv1_1, TLSv1	ALL:!LOW:!aNULL: !EXP:!eNULL	yes

ワイヤ暗号化を介した IP セキュリティ(IPsec)を設定しま す

ONTAPは、転送モードでインターネットプロトコルセキュリティ(IPsec)を使用して、転送中もデータの安全性と暗号化を継続的に確保します。IPSec では、 NFS 、 iSCSI 、 SMB の各プロトコルを含むすべての IP トラフィックを暗号化できます。

ONTAP 9.12.1以降では、フロントエンドホストプロトコルIPsecサポートは、MetroCluster IPおよびMetroCluster ファブリック接続構成で利用できます。 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 以降では、 Pre-Shared Key (PSK; 事前共有キー)または証明書のいずれかを使用して IPSec での認証を行うことができます。以前は、 IPsec でサポートされていたのは PSK だけでした。

ONTAP 9.9.1以降では、IPsecで使用される暗号化アルゴリズムがFIPS 140-2に準拠しています。アルゴリズムは、ONTAP のNetApp Cryptographic Moduleによって生成され、FIPS 140-2認定を継承しています。

ONTAP 9.8以降では、ONTAPでトランスポートモードのIPsecがサポートされます。

IPSec の設定後は、リプレイ攻撃や中間者(MITM)攻撃に対抗するための予防措置を講じて、クライアント と ONTAP 間のネットワークトラフィックを保護します。

NetApp SnapMirror およびクラスタピアリングトラフィックの暗号化では、クラスタピアリング暗号化(CPE)の場合でも、 IPSec 経由でセキュアな転送レイヤセキュリティ(TLS)を使用することを推奨しま す。これは、TLSの方がIPsecよりもパフォーマンスが優れているためです。

クラスタで IPSec 機能が有効になっている場合、ネットワークでトラフィックを処理するには、保護対象の トラフィックと一致する Security Policy Database (SPD)エントリ、および保護の詳細(暗号スイートや 認証方式など)を指定する必要があります。各クライアントには、対応する SPD エントリも必要です。

クラスタで IPSec を有効に設定します

クラスタの IPSec を有効にして、転送中もデータのセキュリティを継続的に確保し、暗号化することができ ます。

手順

1. IPSec がすでに有効になっているかどうかを検出します。

security ipsec config show

結果にが含まれている場合 `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

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た IPsec Enabled: true。

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。

- エンドエンティティ(ONTAPまたはクライアント)の証明書を両側で検証できるように、ONTAPとクラ イアントの両方に相手のCA証明書をインストールする必要があります。
- ・ポリシーに含まれる ONTAP LIF の証明書がインストールされます

(;)

ONTAP LIF は証明書を共有できます。証明書と LIF の間に 1 対 1 のマッピングは必要ありません。

手順

 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

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、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。 security ipsec ca-certificate add コマンドを実行します

サンプルコマンド cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs my_ca_cert

 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 では、トラフィックをネットワーク上に転送する前に 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している場合にも当てはまります。

手順

- 1. を使用します security ipsec policy create コマンドの宛先:
 - a. ONTAP IP アドレスまたは IP アドレスのサブネットを選択して、 IPSec 転送に参加します。
 - 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、 Pre-Shared Key (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. 任意。上位層プロトコル(UDP、TCP、ICMPなど)など、きめ細かなトラフィックパラメータを選択します。)、ローカルポート番号、およびトラフィックを保護するリモートポート番号。対応するパラメータはです protocols、 local-ports および remote-ports それぞれ。

ONTAP IP アドレスとクライアント IP アドレスの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。デフォルトでは、すべてのトラフィックを保護します。

- d. の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 必要な認証方式 のパラメータ。
 - 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 および remote-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、パラメータはオプションです。

ii. PKIを入力する場合は、も入力する必要があります cert-name、 local-identity、 remoteidentity パラメータ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、特殊なIDを入力します。 ANYTHING。

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。詳細については、クラ イアント側のIPsec設定を参照してください。

IPsec ID を使用する

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、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はオプションです。

PKI/ 証明書認証方式の場合、ローカル ID とリモート ID の両方が必須です。IDは、各側の証明書内で認証され、検証プロセスで使用されるIDを指定します。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を使用します ANYTHING。

このタスクについて

ONTAP では、 SPD エントリを変更するか、または SPD ポリシーを作成する際に、 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。

ステップ

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

コマンドの例を示します

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

多数のクライアントで IPSec を利用する必要がある場合、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で IPSec を利用する必要がある場合には、 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。

このタスクについて

ONTAP では、 IPSec が有効な単一の SVM IP アドレスに、多数のネットワーク上にある複数のクライアント を接続できます。これを行うには、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、を指定する必要があります remote-ipsubnets サブネット形式。また、を指定する必要があります remote-identity フィールドに正しいク ライアント側IDを入力します。 サブネット設定で1つ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 Pre-Shared Key (PSK;事前共有キー)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、各クライアントは独自の一意の 証明書または共有証明書を使用して認証できます。ONTAP IPSec は、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、証明書の有効性をチェックします。ONTAP は、証明 書失効リスト (CRL) チェックもサポートしています。

・* 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にSVMのIPsec対応IPアドレスへの接続を許可するに は、を使用します 0.0.0.0/0 ワイルドカードヲシテイスルバアイ remote-ip-subnets フィールド。

また、を指定する必要があります remote-identity フィールドに正しいクライアント側IDを入力しま す。証明書認証の場合は、と入力できます ANYTHING。

また、ときに 0.0.0.0/0 ワイルドカードを使用する場合は、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。例: NFS port 2049。

手順

 (\mathbf{i})

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

コマンドの例を示します

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 -local
-ports port number -local-identity local id -remote-identity remote id

コマンドの例を示します

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の統計情報

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を実行する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。

コマンドの例を示します IKE SA サンプルコマンド:

security ipsec show-ikesa -node hosting_node_name_for_svm_ip

IPSec SA サンプルコマンドおよび出力:

security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

IPSec SA サンプルコマンドおよび出力:

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 _____ __ _____ test34 vs1 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します

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を強化して、ストレージシス テムへの不正アクセスを防止するのに役立ちます。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 、クラスタ間 LIF の特定の IP サービスへのリモー 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。これまでは、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。この機能は、

LIF のサービスポリシーを使用して実行されるようになりました。

- すべてのファイアウォールポリシーが空であり、基盤となるファイアウォールのどのポートも開かない。
 代わりに、LIFの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。
- ファイアウォールポリシーからLIFサービスポリシーに移行するために9.10.1以降にアップグレードしたあとは必要な処理はありません。以前のONTAPリリースで使用されていたファイアウォールポリシーと整合性のあるLIFサービスポリシーが自動的に構築されます。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している場合は、カスタムサービスポリシーを作成するスクリプトのアップグレードが必要になることがあります。

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 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。 NDMP 、 NDMPS 、 RSH 、 DNS 、または SNMP 。NFS や SMB な どのデータプロトコル用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を有効または無効にします
- 現在のファイアウォールサービスの設定を表示しています
- 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してください
- •ファイアウォールポリシーを論理インターフェイスに適用する
- ・既存のファイアウォールポリシーとまったく同一の新しいポリシーを作成する

この機能は、同じ SVM 内でよく似たポリシーを作成するときや、別の SVM にポリシーをコピーすると きに使用できます。

- ファイアウォールポリシーに関する情報を表示する
- ファイアウォールポリシーで使用する IP アドレスとネットマスクを変更する
- ・LIF で使用し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します。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どのように影響する か、および LIF のセキュリティを強化または低下させるためにファイアウォールポリシーをカスタマイズする 方法について理解しておく必要があります。

を使用してLIFを設定する場合 network interface create または network interface modify コマ ンドを入力します。に指定した値です -firewall-policy パラメータは、LIFへのアクセスを許可するサー ビスプロトコルとIPアドレスを決定します。

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。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は、 SSH 、 HTTP 、 HTTPS 、 Telnet 、 NTP 、 NDMP 、 NDMPS 、 RSH 、 DNS 、および SNMP。

すべてのクラスタLIFのファイアウォールポリシーのデフォルトはです "" およびは変更できません。

次の表に、 LIF の作成時にそのロール(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 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権	割り当て先の 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
Mgmt - NFS を管理します	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 RPC サービスがリスンするポートにマッピングします。

ONTAP 9.3 以前では portmap サービスに常にアクセス可能で、 ONTAP 9.4 では ONTAP 9.6 で設定可能にな っており、 ONTAP 9.7 以降では自動的に管理されます。

- ONTAP 9.3 までは、サードパーティ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) へのアクセスが常に許可さ れていました。
- ONTAP 9.4 から ONTAP 9.6 までは、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が廃止されています。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 リリースから ONTAP 9.6 リリースまでの portmap ファイアウォールサービスの設定方法について説明します。

設定によっては、特定のタイプの LIF 、通常は管理 LIF とクラスタ間 LIF でのサービスへのアクセスを禁止で きる場合があります。状況によっては、データ LIF からのアクセスも禁止できます。

想定される動作

ONTAP 9.4 から ONTAP 9.6 への動作は、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可能なサー ビスをLIFタイプ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。影響を受け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 から 9.6 にアップグレードした場合、 ONTAP は、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 サービスを追加します。
- 新しいクラスタ ONTAP 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 を作成するときに、デフォルトのファイアウォールポリシーが割り当てられます。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。LIF にアクセスできるネットワ ークサービスや IP アドレスを変更する場合は、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 てることができます。

このタスクについて

 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 名前 data、 intercluster、 cluster、または `mgmt。

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したり変更したり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、どのサービスタイプでも 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から、 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には、許可されるアドレスのリストにIPv6ワイルドカード::/0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ときは、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、必ず、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 サービスを許可してください。

デフォルトでは、が表示されます intercluster ファイアウォールポリシーは、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NDMPS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や、クラスタ間 LIF の独自のファイアウォー ルポリシーを作成する場合は、許可されるアドレスのリストに各クラスタ間 LIF の IP アドレスを追加し て、 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 の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 および management-ssh LIFサービスは、HTTPSとSSHの管理 アクセスに使用できます。

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

ファイアウォールポリシーに追加するネットワークサービスごとに上記のコマンドを繰り返して、各サービスで許可される IP アドレスを指定できます。

- 2. 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 コマンドを実行します
- 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. 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 コマンドを実行します

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 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 0.0.0.0/0 ndmp ndmps 0.0.0.0/0 ntp 0.0.0.0/0 snmp 0.0.0.0/0 ssh 0.0.0/0 vs1 data http http 10.10.0/16 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 nodel 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 data http vsl datal vs3 data2 data

ファイアウォールサービスおよびポリシーを管理するためのコ マンド

を使用できます system services firewall ファイアウォールサービスを管理する ためのコマンド system services firewall policy ファイアウォールポリシーを 管理するコマンド、および network interface modify LIFのファイアウォール設定 を管理するコマンド。

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しま す	system services firewall modify
ファイアウォールサービスの現在の設定を表示しま す	system services firewall show
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してくだ さい	system services firewall policy create
ファイアウォールポリシーを LIF に適用する	network interface modify -lif lifname -firewall-policy
ファイアウォールポリシーに関連付けられた IP アド レスとネットマスクを変更する	system services firewall policy modify
ファイアウォールポリシーに関する情報を表示する	system services firewall policy show
既存のファイアウォールポリシーとまったく同一の 新しいポリシーを作成します	system services firewall policy clone
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	system services firewall policy delete

詳細については、のマニュアルページを参照してください system services firewall、 system services firewall policy`および `network interface modifyのコマンド "ONTAP 9コマンドリファレンス"。

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。