



『Cisco Intercloud Fabric ファイアウォール コンフィギュレーションガイド、リリース 5.2(1)VSG2(1.1)』

初版：2014年09月30日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



目次

はじめに vii

対象読者 vii

表記法 vii

Microsoft Hyper-V の Cisco Virtual Security Gateway の関連資料 ix

マニュアルに関するフィードバック ix

マニュアルの入手方法およびテクニカル サポート ix

Intercloud Fabric ファイアウォールの概要 1

Intercloud Fabric ファイアウォールに関する情報 1

Intercloud Fabric ファイアウォール 1

概要 1

Intercloud Fabric ファイアウォールの設定 2

製品のアーキテクチャ 3

高速パスの接続タイムアウト 4

信頼できるアクセス 6

ダイナミック（仮想化対応）動作 6

Intercloud Fabric ファイアウォールの導入シナリオ 7

レイヤ 3 モードの Intercloud Fabric ファイアウォール用の VEM インターフェイス 7

Cisco vPath 7

Intercloud Fabric ファイアウォール ネットワーク仮想サービス 7

ネットワークの Intercloud Fabric ファイアウォール設定 7

Intercloud Fabric ファイアウォール設定の概要 7

Intercloud Fabric スイッチ VSM 8

Port Profile 8

Security Profile 8

ファイアウォール ポリシー 9

オブジェクトグループ	9
ゾーン	9
ルール	10
アクション	10
サービス ファイアウォールのロギング	10
Intercloud Fabric ファイアウォールの設定の手順	10
ファイアウォール プロファイルおよびポリシー オブジェクトの設定	13
Intercloud Fabric ファイアウォール ポリシー オブジェクトに関する情報	13
Intercloud Fabric ファイアウォール ポリシー オブジェクトおよびファイアウォール プロファイルに関する情報	13
Intercloud Fabric ファイアウォール ポリシー オブジェクトの設定の前提条件	13
Intercloud Fabric ファイアウォール設定時の注意事項および制約事項	14
デフォルト設定	14
ゾーン	14
ゾーンの例	14
オブジェクトグループ	15
オブジェクトグループの例	15
ルール	15
ルールの例	15
ポリシー	16
ポリシー例	16
Intercloud Fabric ファイアウォール属性	16
属性名表記に関する情報	16
方向属性	16
ニュートラル属性	17
属性クラス	17
ニュートラル属性	17
VM 属性	17
ゾーン属性	19
セキュリティプロファイル	19
サービス ファイアウォールのロギングの設定	20

Intercloud Fabric ファイアウォール設定の確認	20
コマンドライン インターフェイスの使用	23
CLI プロンプトの概要	23
コマンド モード	24
コマンド モードに関する情報	24
コマンド モードの概要	24
特殊文字	24
キーストローク ショートカット	25
コマンドの省略形	27
ヘルプの使用	28
構文エラーの分離および状況依存ヘルプ	28
システム管理の設定	31
Intercloud Fabric ファイアウォール設定の確認	31
インターフェイス コンフィギュレーションの表示	33
Intercloud Fabric ファイアウォール インスタンスの表示	34
ファイル システム内の移動	35
ファイル システムの指定	35
現在の作業ディレクトリの特定	36
ディレクトリの変更	36
ファイル システム内のファイルの一覧表示	37
ファイルをコピーするために使用できるファイル システムの特定	38
タブ補完の使用	39
ファイルのコピーとバックアップ	40
ディレクトリの作成	41
既存のディレクトリの削除	42
ファイルの移動	42
ファイルまたはディレクトリの削除	43
ファイルの圧縮	44
ファイルの圧縮解除	45
コマンド出力のファイル保存	46
ファイルの表示	46
現在のユーザ アクセスの表示	48

ユーザへのメッセージ送信	48
SNMP の設定	51
SNMP に関する情報	51
SNMP 機能の概要	51
SNMP 通知	52
SNMPv3	52
SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル	53
ユーザベースのセキュリティ モデル	53
コマンドライン インターフェイス (CLI) および SNMP ユーザの同期	54
グループベースの SNMP アクセス	55
注意事項と制約事項	55
SNMP の設定	55
SNMP の設定確認	56
MIB	57



はじめに

ここでは、次の項について説明します。

- [対象読者](#), [vii ページ](#)
- [表記法](#), [vii ページ](#)
- [Microsoft Hyper-V の Cisco Virtual Security Gateway の関連資料](#), [ix ページ](#)
- [マニュアルに関するフィードバック](#), [ix ページ](#)
- [マニュアルの入手方法およびテクニカル サポート](#), [ix ページ](#)

対象読者

本書は、Cisco Nexus デバイス の設定と保守を行う、ネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体を使用できない場合に使用されます。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

Microsoft Hyper-V の Cisco Virtual Security Gateway の関連資料

ここでは、Microsoft Hyper-V および関連製品の Cisco Virtual Security Gateway で利用可能なマニュアルを示します。

Cisco Virtual Security Gateway に関するマニュアル

『Cisco Virtual Security Gateway for Microsoft Hyper-V』は http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html から入手可能です。

『Cisco Virtual Security Gateway for Microsoft Hyper-V Release Notes』

『Cisco Virtual Security Gateway for Microsoft Hyper-V Installation Guide』

『Cisco Virtual Security Gateway for Microsoft Hyper-V Configuration Guide』

『Cisco Virtual Security Gateway for Microsoft Hyper-V Troubleshooting Guide』

『Cisco Virtual Security Gateway for Microsoft Hyper-V Command Reference』

『Cisco vPath and vServices Reference Guide for Microsoft Hyper-V』

Microsoft Hyper-V ソフトウェアの Nexus 1000V シリーズ NX-OS の関連資料

『Cisco Nexus 1000V Series Switch for Microsoft Hyper-V』のマニュアルは、Cisco.com の次の URL で入手できます。

http://www.cisco.com/en/US/products/ps13056/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載漏れに関する報告は、vsg-docfeedback@cisco.com に送信してください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html> から入手できます。

『*What's New in Cisco Product Documentation*』はシスコの新規および改訂版の技術マニュアルの一覧を提供するもので、RSS フィードとして購読できます。また、リーダーアプリケーションを使用すると、コンテンツがデスクトップに直接配信されるようになります。RSS フィードは無料のサービスです。



第 1 章

Intercloud Fabric ファイアウォールの概要

この章の内容は、次のとおりです。

- [Intercloud Fabric ファイアウォールに関する情報, 1 ページ](#)
- [ネットワークの Intercloud Fabric ファイアウォール設定, 7 ページ](#)

Intercloud Fabric ファイアウォールに関する情報

Intercloud Fabric ファイアウォール

Intercloud Fabric (ICF) ファイアウォール (VSG) は、仮想データセンターおよびクラウド環境へ信頼できるアクセスを提供する仮想ファイアウォールアプライアンスです。管理者はホスト上でサービス VM として ICF ファイアウォールをインストールし、セキュリティプロファイルとファイアウォールポリシーで設定できます。これにより、VM セグメンテーションおよび他のファイアウォール機能を提供し、VM へのアクセスを保護します。

概要

Intercloud Fabric (ICF) ファイアウォールは、動的なポリシーベース操作、トランスペアレントモビリティの強化および高密度マルチテナント機能のスケールアウト展開の要件を満たしながら、クラウドプロバイダー環境でセキュアな仮想化データセンターへの信頼できるアクセスを提供する仮想アプライアンスです。ICF ファイアウォールによって、信頼ゾーンへのアクセスが確立されたセキュリティポリシーにより確実に制御および監視されるようになります。ICF ファイアウォールにより、ワークロード仮想化、企業のセキュリティポリシーおよび業界規制の順守の強化、および簡素化されたセキュリティ監査機能といったメリットが提供されます。

ICF ファイアウォールは、クラウドサービスルータ (CSR) またはクラウド VM のパブリックインターフェイスを介して VM にアクセスしようとする認可されていないインターネットユーザなどの潜在的に有害なネットワークトラフィックや、サイト間のセキュアなトンネル経由でアクセ

スしようとする認可されていない内部ユーザからクラウド環境の仮想マシン (VM) を保護します。

Intercloud 環境で ICF ファイアウォールを導入することで、顧客は企業のセキュリティポリシーを拡張してパブリッククラウドで動作しているアプリケーションワークロードを保護することができます。また、ICF ファイアウォールは、Intercloud 環境の 3 階層型アプリケーションのサポートを通じて、VM グループ間の論理的な分離も提供します。セキュリティ要件に基づいて、VM を論理グループの一部として定義することができ、ICF ファイアウォールを VM グループに適用することができます。

Intercloud 環境の ICF ファイアウォールは、クラウドアプリケーションの仮想マシン (VM) および eVM と cVM 間の通信をセキュリティで保護します。ICF ファイアウォールは、次の利点を提供します。

- 信頼できるマルチテナントアクセス：法規制の遵守を強化し、監査を簡素化するための、マルチテナント (スケールアウト) 環境におけるコンテキスト対応セキュリティポリシーによるゾーンベースの制御およびモニタリング。セキュリティポリシーは、セキュリティプロファイルテンプレートへと組織され、多くの ICF ファイアウォールの管理および配置を簡素化します。
- ダイナミック操作：VM がインスタンス化する間のセキュリティテンプレートおよび信頼ゾーンのオンデマンドプロビジョニングと、プライベートクラウドとパブリック (Amazon) クラウド間で VM の移行が発生するときのトランスペアレントモビリティの強化およびモニタリング。
- 中断しない管理：セキュリティ全体およびサーバチーム全体における管理分離。コラボレーションを提供し、管理者によるエラーを削除し、監査を簡素化します。

ICF ファイアウォールでは次のことが実行されます。

- 仮想化データセンターの仮想マシンのセキュアなセグメンテーション。
- ダイナミックなデータセンターのセキュリティを維持します。
- 仮想化環境の監査プロセスを簡略化します。
- プライベート/パブリック クラウド コンピューティング環境で仮想化ワークロードを安全に導入することによりコストを削減します。

Intercloud Fabric ファイアウォールの設定

Intercloud Fabric (ICF) ファイアウォールは、次の設定で使用可能です。

表 1: ICF ファイアウォール設定

ICF ファイアウォールモデル	メモリ	CPU 速度	仮想 CPU の数	ネットワークアダプタ
Medium	2 GB	1.0 GHz	1	2

製品のアーキテクチャ

Intercloud Fabric (ICF) ファイアウォールは、クラウド環境 (Amazon や ICFPP を使用したクラウドプロバイダー) で Intercloud スイッチとともに動作し、ICS で動作する Intercloud スイッチ仮想イーサネット モジュール (VEM) に組み込まれる Cisco 仮想ネットワーク サービス データパス (vPath) を利用します。

Cisco vPath は、保護された VM トラフィックをテナントの ICF ファイアウォールにリダイレクトします。ICF ファイアウォールでは初期パケットの処理が行われ、ポリシーが評価および適用されます。ポリシーに関する決定が下されると、ICF ファイアウォールは、残りのパケットのポリシーの適用を Cisco vPath にオフロードします。Cisco vPath は次の機能をサポートします。

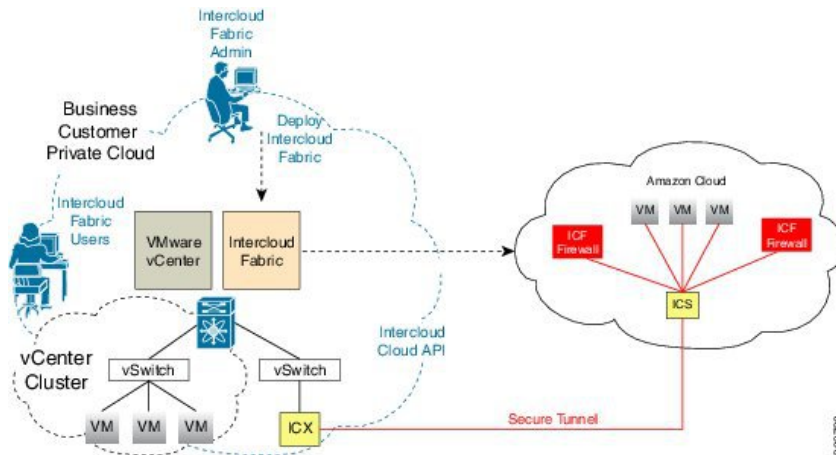
- インターセプションとリダイレクション：指定された ICF ファイアウォールテナントへのテナント対応フロー分類とその後のリダイレクション
- 高速パスのオフロード：ICF ファイアウォールによって vPath へオフロードされるフローのテナントごとのポリシーの適用

ICF ファイアウォールと Intercloud スイッチ仮想イーサネット モジュール (VEM) には次の利点があります。

- 効率的な配置：各 ICF ファイアウォールは、クラウド VM へのアクセスと、Intercloud スイッチでのクラウド VM 間のトラフィックを保護します。
- パフォーマンスの最適化：高速パスを 1 つ以上の Intercloud スイッチ VEM vPath モジュールにオフロードすることで、ICF ファイアウォールは分散型 Cisco vPath ベースの適用によりネットワーク パフォーマンスを向上させます。

- 運用の簡素化：ICF ファイアウォールは、icfCloud 1 つあたり 1 つのファイアウォールでワンアーム モードで透過的に挿入できます。ゾーン拡張は、仮想アプライアンスに限定されている vNIC ではなく、セキュリティ プロファイルに基づきます。

図 1：Intercloud Fabric ファイアウォールの配置トポロジ



高速パスの接続タイムアウト

保護された VM のパケットを初めて受信すると VEM は、Intercloud Fabric (ICF) ファイアウォールにそのパケットをリダイレクトし、実行するアクションを決定します（例：許可、ドロップ、リセットなど）。アクションが決定された後、ICF ファイアウォールと VEM の両方が接続情報およびアクションを一定期間保存します。この間、この接続のためのパケットは、追加のポリシー検索なしで同じアクションに従います。VEM/vPath の接続は、ICF ファイアウォールへのパケットのリダイレクションを回避するため、高速パス接続と呼ばれます。トラフィックとアクションに応じて、接続が高速パスモードを継続する時間は異なります。次の表に、高速パスモード接続のタイムアウトの詳細を示します。

表 2: 高速パスの接続タイムアウト

プロトコル	接続状態	タイムアウト
TCP	FIN および ACKACK で閉じる	VEM : 4 秒
		ファイアウォール : 4 秒
	RST で閉じる	VEM : 4 秒
		ファイアウォール : 4 秒
	アクションのドロップ	VEM : 4 秒
		ファイアウォール : 4 秒
	アクションのリセット	VEM : 4 秒
		ファイアウォール : 4 秒
	Idle	VEM : 36 ~ 60 秒
		ファイアウォール : 630 ~ 930 秒
UDP	アクションのドロップ	VEM : 4 秒
		ファイアウォール : 4 秒
	アクションのリセット	VEM : 4 秒
		ファイアウォール : 4 秒
	Idle	VEM : 8 ~ 12 秒
		ファイアウォール : 240 ~ 360 秒
	宛先到達不能	VEM : 4 秒
		ファイアウォール : 4 秒

プロトコル	接続状態	タイムアウト
L3/ICMP	アクションのドロップ	VEM : 2 秒
		ファイアウォール : 2 秒
	アクションのリセット	VEM : 2 秒
		ファイアウォール : 2 秒
	Idle	VEM : 8 ~ 12 秒
		ファイアウォール : 16 ~ 24 秒

信頼できるアクセス

Intercloud スイッチが導入されたクラウド環境に Intercloud Fabric (ICF) ファイアウォールを透過的に挿入できます。ICF ファイアウォールの 1 つ以上のインスタンスは、テナントごとに配置されます。これにより多くのテナントからなる大規模な配置が可能になります。テナントは分離されるので、トラフィックがテナントの境界を越えることはありません。テナントレベルで ICF ファイアウォールを配置できます。

VM は特定のテナントについてインスタンス化されるため、VM とセキュリティプロファイルおよびゾーンメンバーシップとの関連付けは、Intercloud スイッチポートプロファイルとのバインディングを介してただちに実行されます。各 VM は、インスタンス化が行われると論理的信頼ゾーンに配置されます。セキュリティプロファイルには、各ゾーンを出入りするトラフィックのアクセスポリシーを設定するコンテキストウェアナールールセットが含まれます。ゾーンからゾーンへのトラフィックに加え、外部からゾーン（およびゾーンから外部）へのトラフィックにもセキュリティプロファイルが適用されます。ゾーンベースの適用は VLAN 内でも行うことができ、VLAN は頻繁にテナントの境界を識別します。ICF ファイアウォールはアクセスコントロールルールを評価し、設定されている場合は、Intercloud スイッチ VEM vPath モジュールへの適用をオフロードします。ICF ファイアウォールはアクセスを許可または拒否できます。また、オプションのアクセスログが生成される場合もあります。ICF ファイアウォールは、アクセスログを使用したポリシーベースのトラフィックモニタリング機能も提供します。

ダイナミック（仮想化対応）動作

仮想化環境はダイナミックです。つまり、追加、削除、変更の操作がテナント間、および VM 間で頻繁に行われます。Intercloud スイッチ（および vPath）と動作する Intercloud Fabric (ICF) ファイアウォールは、ダイナミック VM 環境をサポートします。通常、ICF ファイアウォールを備えた ICF サービスコントローラでテナントを作成すると、信頼ゾーン定義およびアクセスコントロールルールを含む関連セキュリティプロファイルが定義されます。各セキュリティプロファイルは、Intercloud スイッチポートプロファイルにバインドされます。ポートプロファイルが一

意にセキュリティプロファイルと VM ゾーンメンバーシップを参照するため、セキュリティ制御はただちに適用されます。

Intercloud Fabric ファイアウォールの導入シナリオ

現在のリリースは、レイヤ3モードでの Intercloud Fabric (ICF) ファイアウォールの導入をサポートしています。VEM と ICF ファイアウォールは、Intercloud Fabric サービス インターフェイスと呼ばれる特別な仮想ネットワーク インターフェイスを介して互いに通信します。

レイヤ3モードの Intercloud Fabric ファイアウォール用の VEM インターフェイス

サービス インターフェイスは、レイヤ3モードの Intercloud Fabric ファイアウォールと通信するために Intercloud スイッチで作成されます。

ICF ファイアウォール宛てのカプセル化されたトラフィックが L3 インターフェイス以外の別のサブネットに接続されている場合、VEM はホストルーティングテーブルを使用しません。代わりに、L3 サービス インターフェイスは、ICF ファイアウォールの IP アドレスに対して ARP を開始します。

Cisco vPath

vPath は、Intercloud スイッチ VEM に組み込まれます。これは VM から VM へのトラフィックを代行受信して、このトラフィックを Intercloud Fabric ファイアウォールにリダイレクトします。詳細については、『*Cisco vPath and vServices Reference Guide for Intercloud Fabric*』を参照してください。

Intercloud Fabric ファイアウォール ネットワーク仮想サービス

Intercloud Fabric ネットワーク仮想サービス (vservice) は、vPath を使用して Intercloud スイッチによりサポートされます。信頼できるマルチテナントアクセスが提供されます。詳細については、『*Cisco vPath and vServices Reference Guide for Intercloud Fabric*』を参照してください。

ネットワークの Intercloud Fabric ファイアウォール設定

Intercloud Fabric ファイアウォール設定の概要

クラウド VSM で Intercloud Fabric (ICF) ファイアウォールを適用する場合は、クラウド VSM を設定する必要があります。



(注) ICF ファイアウォールを設定する方法については、『Cisco vPath and vServices Reference Guide for Intercloud Fabric』を参照してください。

Intercloud Fabric スイッチ VSM

VSM は、論理的なモジュラ スイッチです。1 つの VSM が複数の VEM を制御します。VSM は、物理的なラインカードではなく、ICS 内のソフトウェアで実行される VEM をサポートします。ICS のすべての VEM の設定は VSM を通して実行され、自動的に VEM に伝播されます。

Port Profile

Intercloud Fabric スイッチのポート プロファイルは、各 VM に対するネットワーク パラメータを動的にプロビジョニングします。Intercloud Fabric スイッチで、ポート プロファイルはインターフェイスを設定するために使用されます。ポート プロファイルは、複数のインターフェイスに割り当てることができ、すべてのインターフェイスは同じポート プロファイル設定を継承します。ポート プロファイルに対する変更は、そのポート プロファイルに関連付けられた VM インターフェイスに自動的に伝播されます。

vservice および org コマンドを使用してセキュリティ プロファイルおよび Intercloud Fabric ファイアウォール ノードとバインドする場合、VM ポート プロファイルは Intercloud Fabric ファイアウォールによって提供される (VM セグメンテーションなどのための) セキュリティ サービスを設定するために使用できます。

Security Profile

Intercloud Fabric スイッチのポート プロファイルは、各 VM に対するネットワーク パラメータを動的にプロビジョニングします。同じポリシーのプロビジョニングは、VM がポート プロファイルに接続された場合、各 VM がネットワーク サービスポリシーとダイナミックにプロビジョニングされるようにネットワーク サービスの設定情報を伝達します。このプロセスは、関連しているアクセス コントロール リスト (ACL) またはポート プロファイルの Quality of Service (QoS) ポリシーと同様です。ネットワーク サービスの設定に関する情報は、セキュリティ プロファイルと呼ばれる独立したプロファイル内に作成され、ポート プロファイルに接続されます。セキュリティ管理者は、Cisco Prime NSC にセキュリティ プロファイルを作成し、これをネットワーク管理者が VSM の適切なポート プロファイルに関連付けます。

セキュリティ プロファイルは、ポリシーの記述に使用できるカスタム属性を定義します。特定のポート プロファイルに関連付けられたすべての VM は、そのポート プロファイルに関連付けられたセキュリティ プロファイルで定義されたファイアウォールポリシーおよびカスタム属性を継承します。各カスタム属性は state = CA のように名前と値のペアで設定されます。ネットワーク管理者はまた、特定のポート プロファイルに関連付けられている Intercloud Fabric (ICF) ファイアウォールをバインドします。ポート プロファイルに関連付けられた ICF ファイアウォールは、そのポート プロファイルにバインドされるアプリケーション VM のネットワーク トラフィックに対してファイアウォール ポリシーを適用します。トラフィックがサービス プロファイルにバイン

ドされている場合、そのサービスプロファイルに関連付けられたポリシーが実行されるように、サービスプロファイル固有のポリシーをバインドすることもできます。サービスプレーンおよび管理プレーンは、両方ともマルチテナント機能の要件をサポートします。異なるテナントは、独自の ICF ファイアウォールを設定できます。

ファイアウォールポリシー

Intercloud Fabric (ICF) ファイアウォールの主要コンポーネントはポリシー エンジンです。ポリシー エンジンは、ICF ファイアウォールで受信したネットワークトラフィックをフィルタリングする設定としてポリシーを使用します。

ポリシーは、一連の間接的な関連付けを使用して ICF ファイアウォールにバインドされます。セキュリティ管理者は、セキュリティプロファイルを設定すると、セキュリティプロファイル内のポリシー名を参照できます。セキュリティプロファイルは、ICF ファイアウォールへのリファレンスを持つポートプロファイルに関連付けられます。

ポリシーは、次のポリシー オブジェクトのセットを使用して構築されます。

- オブジェクトグループ
- ゾーン
- ルール
- アクション

オブジェクトグループ

オブジェクトグループは、属性に関連する条件のセットです。オブジェクトグループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、オブジェクトグループ条件で使用される属性は、方向付けされず、ニュートラルである必要があります。オブジェクトグループは、ファイアウォールルールの記述を支援するセカンダリポリシー オブジェクトです。ルール条件は、演算子を使用することによりオブジェクトグループを参照できます。

ゾーン

ゾーンは、VM の論理グループまたはホストです。ゾーンは、ゾーン名を使用したゾーン属性に基づくポリシーの記述を許可することにより、ポリシーの記述を簡素化できます。ゾーン定義により、ゾーンに VM がマッピングされます。論理グループの定義は、VM に関連付けられた属性に基づくことができます。ゾーン定義は条件ベースのサブネットおよびエンドポイントの IP アドレスとして記述できます。

ゾーンおよびオブジェクトグループは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は、方向付けされず、ニュートラルである必要があります。

ルール

ファイアウォールルールは複数の条件とアクションで構成できます。ルールは、トラフィックをフィルタリングする条件としてポリシーで定義できます。ポリシーエンジンは、Intercloud Fabric ファイアウォールで受信したネットワークトラフィックをフィルタリングする設定としてポリシーを使用します。ポリシーエンジンは、ネットワークトラフィックをフィルタリングする2種類の条件一致モデルを使用します。

AND モデル：ルール内のすべての属性が一致する場合、ルールは `matched` に設定されます。

OR モデル：属性は5つの異なるタイプのカラムに分類されます。trueになるルールの場合、各カラムで少なくとも1つの条件が true である必要があります。OR モデルの5つのカラムは下記のとおりです。

- 送信元カラム：送信元ホストを識別するための属性。
- 宛先カラム：宛先ホストを識別するための属性。
- サービスカラム：宛先ホストでサービスを識別するための属性。
- Ether タイプカラム：リンクレベルプロトコルを識別するための属性。
- 送信元ポートカラム：送信元ポートを識別するための属性。

アクション

アクションはポリシー評価の結果です。指定したルール内で、次のアクションを1つまたは複数定義して関連付けることができます。

- Permit
- Drop
- Reset
- Log
- Inspection

サービス ファイアウォールのロギング

サービスファイアウォールのログは、ポリシーのテストおよびデバッグを行うツールです。ポリシーの評価中に、ポリシーエンジンによりポリシー評価のポリシー結果が表示されます。

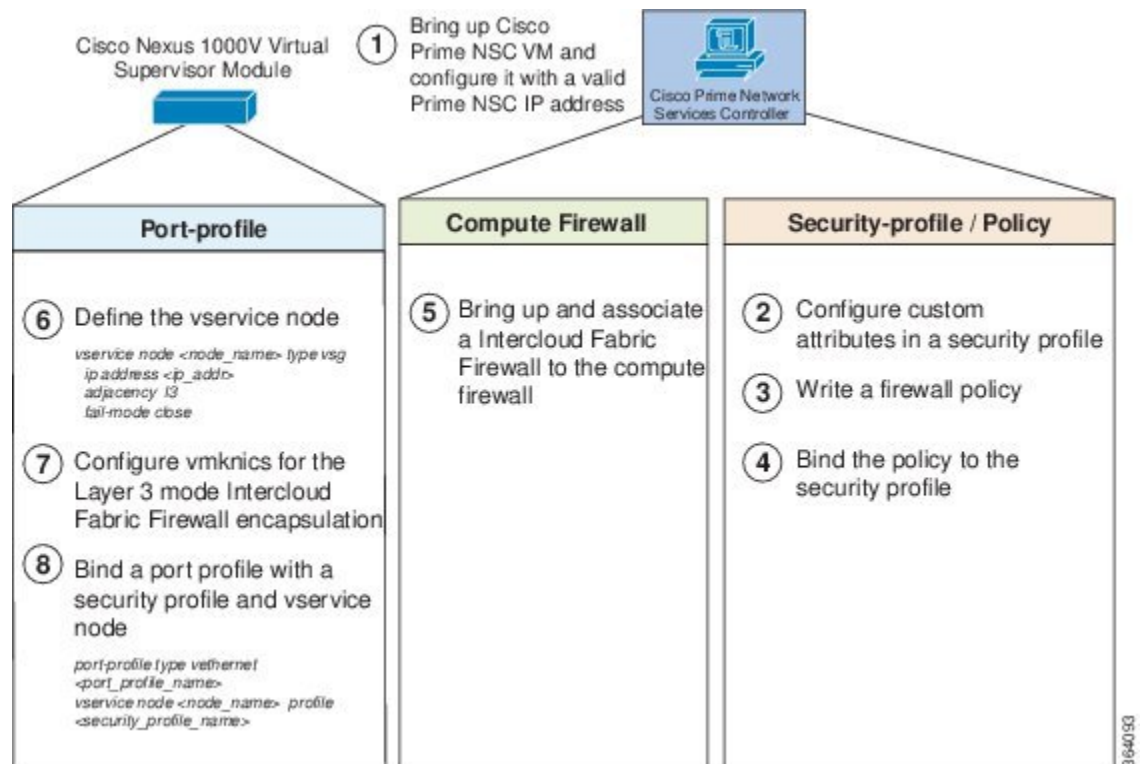
Intercloud Fabric ファイアウォールの設定の手順

ここでは、Intercloud Fabric (ICF) ファイアウォールを設定する際に管理者が従うべき手順の概要を説明します。

- 1 ICF をインストールしセットアップします。

- 2 ICF を介してインフラストラクチャウィザードを実行し、ICF サービスコントローラと cVSM を起動します。
- 3 ICF から icfCloud を導入します。 [ICF Firewall services] チェックボックスをオンにして、サービスインターフェイスの詳細を指定します。
- 4 オブジェクトグループ、ゾーン、ルール、条件、アクション、ポリシーなどのポリシーオブジェクトを使用して、ICF サービスコントローラ上でファイアウォールポリシーを記述します。
- 5 ファイアウォールポリシーを作成した後で、先に Cisco Prime NSCCisco Prime NSC で作成されたセキュリティプロファイルにポリシーをバインドします。
- 6 ICF サービスコントローラで ICF ファイアウォールを導入します。
- 7 ICF を介して ICS 上でサービスインターフェイスを設定します。
- 8 同じ VLAN/ネットワークに Intercloud Fabric データおよびサービスインターフェイスを設定します。
- 9 セキュリティプロファイルとファイアウォールポリシーが設定されると、ICF 上のポートプロファイル管理インターフェイスを介して ICF ファイアウォール提供のアクセス保護を要求する VM ポートプロファイルに、セキュリティプロファイルとサービスノードをバインドできます。

図 2: Intercloud Fabric ファイアウォールのレイヤ 3 設定フロー





第 2 章

ファイアウォール プロファイルおよびポリシー オブジェクトの設定

この章の内容は、次のとおりです。

- [Intercloud Fabric ファイアウォール ポリシー オブジェクトに関する情報, 13 ページ](#)
- [サービス ファイアウォールのロギングの設定, 20 ページ](#)
- [Intercloud Fabric ファイアウォール設定の確認, 20 ページ](#)

Intercloud Fabric ファイアウォール ポリシー オブジェクトに関する情報

ここでは、Cisco Prime ネットワーク サービス コントローラ (Prime NSC) を使用して、Intercloud Fabric ファイアウォールでファイアウォール ポリシー オブジェクトを設定し管理する方法について説明します。



(注) Cisco PNSC を通じてのみ、Intercloud Fabric ファイアウォールを設定できます。現在は、ファイアウォール ポリシー オブジェクトの帯域外の設定と管理はサポートしていません。

Intercloud Fabric ファイアウォール ポリシー オブジェクトおよびファイアウォール プロファイルに関する情報

Intercloud Fabric ファイアウォール ポリシー オブジェクトの設定の前提条件

Intercloud Fabric (ICF) ファイアウォール ポリシー オブジェクトには次の前提条件があります。

- ICF からデータと管理ポート プロファイルを作成する。
- PNSC から Intercloud Fabric ファイアウォールをインスタンス化する。

Intercloud Fabric ファイアウォール設定時の注意事項および制約事項

Intercloud Fabric (ICF) ファイアウォール (VSG) ポリシー オブジェクトおよびファイアウォール ポリシーには次の設定時の注意事項と制限事項があります。

- 管理 VLAN はクラウドに拡張する必要があります。
- 異なる IP サブネットで ICF ファイアウォールの管理およびデータ インターフェイスを設定します。

デフォルト設定

表 3: *Intercloud Fabric* ファイアウォール (VSG) のデフォルトのパラメータ設定

パラメータ	デフォルト
ルール ポリシー オブジェクト	drop

ゾーン

ゾーンは、VM の論理グループまたはホストです。ゾーンは、ゾーン名を使用したゾーン属性に基づくポリシーの記述を許可することにより、ポリシーの記述を簡素化できます。ゾーン定義により、ゾーンに VM がマッピングされます。論理グループの定義は、VM 属性やネットワーク属性など、VMに関連付けられた属性に基づくことができます。ゾーン定義は条件ベースのサブネットおよびエンドポイントの IP アドレスとして記述できます。

ゾーンおよびオブジェクトグループは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は、方向付けされず、ニュートラルである必要があります。

ゾーンの例

次に、ネットワークのゾーンを表示する例を示します。

```
vsg# show running-config zone zone1
zone zone1
cond-match-criteria: match-any
condition 1 net.ip-address eq 1.1.1.1
condition 2 net.port eq 80
```

オブジェクト グループ

オブジェクトグループは、属性に関連する条件のセットです。オブジェクトグループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、オブジェクトグループ条件で使用される属性は、方向付けされず、ニュートラルである必要があります。オブジェクトグループは、ファイアウォールルールの記述を支援するセカンダリ ポリシー オブジェクトです。ルール条件は、演算子を使用することによりオブジェクトグループを参照できます。

オブジェクトグループの例

次に、ネットワークのオブジェクトグループを表示する例を示します。

```
vsg# show running-config object-group g1
object-group g1 net.port
match 10 in-range protocol 6 port 10 30
match 11 eq protocol 6 port 21 inspect ftp
```

ルール

ファイアウォールルールは複数の条件とアクションで構成できます。ルールは、トラフィックをフィルタリングする条件としてポリシーで定義できます。ポリシーエンジンは、Intercloud Fabric ファイアウォール (VSG) で受信したネットワークトラフィックをフィルタリングする設定としてポリシーを使用します。ポリシーエンジンは、ネットワークトラフィックをフィルタリングする2種類の条件一致モデルを使用します。

AND モデル：ルール内のすべての属性が一致する場合、ルールは **matched** に設定されます。

OR モデル：属性は5つの異なるタイプのカラムに分類されます。trueになるルールの場合、各カラムで少なくとも1つの条件が true である必要があります。OR モデルの5つのカラムは下記のとおりです。

- 送信元カラム：送信元ホストを識別するための属性。
- 宛先カラム：宛先ホストを識別するための属性。
- サービスカラム：宛先ホストでサービスを識別するための属性。
- Ether タイプカラム：リンクレベルプロトコルを識別するための属性。
- 送信元ポートカラム：送信元ポートを識別するための属性。

ルールの例

次に、ネットワークのルールを表示する例を示します。

```
vsg# show running-config rule r2
rule r2
cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.zone.name eq z1@r2
  service/protocol-attribute
    condition 11 net.service eq protocol 6 port 21 inspect ftp
action permit
```

ポリシー

ポリシーは Intercloud Fabric (ICF) ファイアウォール (VSG) でネットワーク トラフィックに適用されます。ICF ファイアウォールで動作する主要コンポーネントはポリシーエンジンです。ポリシーエンジンは、ICF ファイアウォールで受信されるネットワーク トラフィックに対して適用された場合に、ポリシーを設定として取得し、実行します。ポリシーは、次のポリシーオブジェクトのセットを使用して構築されます。

- ルール
- 条件
- アクション
- オブジェクト グループ
- ゾーン

ポリシーは、一連の間接的な関連付けを使用して ICF ファイアウォールにバインドされます。セキュリティ管理者は、セキュリティプロファイルを設定すると、セキュリティプロファイル内のポリシー名を参照できます。セキュリティプロファイルは、ICF ファイアウォールへのリファレンスを持つポートプロファイルに関連付けられます。

ポリシー例

次に、**show running-config** コマンド出力にポリシーが表示される例を示します。

```
vsg# show running-config policy p2@root/T1
policy p2@root/T1
  rule r2 order 10
```

次に、**show running-config** コマンド出力に条件が表示される例を示します。

```
condition 1 dst.net.ip-address eq 2.2.2.2
condition 2 src.net.ip-address eq 1.1.1.1
```

次に、**show running-config** コマンド出力にアクションが表示される例を示します。

```
action permit
```

Intercloud Fabric ファイアウォール属性

ここでは、Intercloud Fabric ファイアウォール (VSG) 属性について説明します。

属性名表記に関する情報

方向属性

ファイアウォール ポリシーは、着信パケットまたは発信パケットに対して方向付けられています。ルール条件内の属性は、送信元または宛先のいずれかに関連するように指定されたものが重要です。src.、dst.のようなプレフィックス、または属性名は、方向付けに使用されます。

ニュートラル属性

オブジェクトグループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は方向付けされません。方向付けされていない属性（src. または dst. などの方向プレフィックスを提供しない）は、ニュートラル属性と呼ばれます。

異なる方向の2つのルール条件は同じオブジェクトグループ定義を共有できます。オブジェクトグループで使用されるニュートラル属性と net.ip-address は、src.net.ip-address および dst.net.ip-address のような異なるルールで使用される方向属性と関連付けることができます。

属性クラス

属性は、ポリシー ルールおよび条件の設定、またはゾーン定義で使用されます。

ニュートラル属性

オブジェクトグループおよびゾーンは異なる方向のさまざまなルール間で共有されるため、ゾーンで使用される属性は方向付けされません。方向付けされていない属性（src. または dst. などの方向プレフィックスを提供しない）は、ニュートラル属性と呼ばれます。

異なる方向の2つのルール条件は同じオブジェクトグループ定義を共有できます。オブジェクトグループで使用されるニュートラル属性と net.ip-address は、src.net.ip-address および dst.net.ip-address のような異なるルールで使用される方向属性と関連付けることができます。

VM 属性

VM 属性は VM インフラストラクチャに関連し、次のクラスの VM 属性があります。

- 仮想インフラストラクチャ属性：これらの属性は Intercloud Fabric から取得され、名前にマッピングされます。
- ポート プロファイル属性：これらの属性は、ポート プロファイルに関連付けられます。
- カスタム属性：これらの属性は、サービス プロファイルで設定できます。

次の表に、Intercloud Fabric ファイアウォール（VSG）によってサポートされる VM 属性を示します。

説明	名前
VM の名前	src.vm.name dst.vm.name vm.name (注) vm.name はニュートラル属性です。

説明	名前
ゲスト OS のフルネーム (バージョン含む)	src.vm.os-fullname dst.vm.os-fullname vm.os-fullname (注) vm.os-fullname はニュートラル属性です。
特定の vNIC に関連付けられたポートプロファイルの名前	src.vm.portprofile-name dst.vm.portprofile-name vm.portprofile-name (注) vm.portprofile-name はニュートラル属性です。
関連付けられたポートグループのセキュリティプロファイルからのカスタム属性。 (注) 一意のカスタム属性 xxx ごとに、合成された属性名は src.vm.custom.xxx または dst.vm.custom.xxx となります。ポリシーは合成された属性名を使用します。	src.vm.custom.xxx dst.vm.custom.xxx vm.custom.xxx (注) vm.custom.xxx はニュートラル属性です。

カスタム VM 属性は、サービス プロファイルの下で設定できるユーザ定義の属性です。

次に、ICF ファイアウォールの VM 属性を確認する例を示します。

```
firewall(config)# show vsg vm
VM uuid          : 47592090-c9c2-5e67-f044-9d6a39dc1696
VM attributes :
  name           : didata1-cvm
  os-fullname    : rhel 6.2 (64bit)

Zone(s) :

-----
VM uuid          : 503ee75f-437b-1fa0-f0f4-fe0da53bab7a
VM attributes :
  host-name      : 10.36.6.9
  name           : windowsvm-migrate
  os-fullname    : microsoft windows server 2003 (32-bit)
  os-hostname   : sg-w2k-rv-1
  resource-pool  : resources
  tools-status   : installed
```

ゾーン属性

表 4: *Intercloud Fabric* ファイアウォールでサポートされるゾーン属性

説明	名前
ゾーン名を指定します。これは複数値属性で、複数のゾーンに同時に属することができます。	src.zone.name dst.zone.name zone.name (注) zone.name はニュートラル属性です。

セキュリティ プロファイル

セキュリティプロファイルは、ポリシーの記述に使用できるカスタム属性を定義します。特定のポートプロファイルのタグが付いたすべてのVMは、そのポートプロファイルに関連付けられたセキュリティプロファイルで定義されたファイアウォールポリシーおよびカスタム属性を継承します。各カスタム属性は、state = CA のように名前と値のペアとして設定されます。

次に、Intercloud Fabric (ICF) ファイアウォールのセキュリティ プロファイルを確認する例を示します。

```
firewall(config-vnm-policy-agent)# show vsg security-profile table
-----
Security-Profile Name VNSP ID Policy Name
-----
default@root 1 default@root
sp10@root/tenant_d3338 9 ps9@root/tenant_d3338
sp9@root/tenant_d3338 10 ps9@root/tenant_d3338
sp2@root/tenant_d3338 11 ps1@root/tenant_d3338
sp1@root/tenant_d3338 12 ps1@root/tenant_d3338
```

次に、ICF ファイアウォールのセキュリティ プロファイルを確認する例を示します。

```
firewall(config-vnm-policy-agent)# show vsg security-profile
VNSP : sp10@root/tenant_d3338
VNSP id : 9
Policy Name : ps9@root/tenant_d3338
Policy id : 3
Custom attributes :
  vnsporg : root/tenant_d3338
VNSP : default@root
VNSP id : 1
Policy Name : default@root
Policy id : 1
Custom attributes :
  vnsporg : root
VNSP : sp1@root/tenant_d3338
VNSP id : 12
Policy Name : ps1@root/tenant_d3338
Policy id : 2
Custom attributes :
  vnsporg : root/tenant_d3338
location : losangeles
color9 : test9
```

```

color8 : test8
color7 : test7
color6 : test6
color5 : test5
color4 : test4
color3 : test3
color2 : test2
color13 : test13
color12 : test12
color11 : test11
color10 : test10
color1 : test1
color : red
VNSP : sp2@root/tenant_d3338
VNSP id : 11
Policy Name : ps1@root/tenant_d3338
Policy id : 2
Custom attributes :
  vnsporg : root/tenant_d3338
  location : sanjose
  color : blue
VNSP : sp9@root/tenant_d3338
VNSP id : 10
Policy Name : ps9@root/tenant_d3338
Policy id : 3
Custom attributes :
  vnsporg : root/tenant_d3338

```

サービス ファイアウォールのログギングの設定

『』の「Enabling Global Policy-Engine Logging」の項を参照してください。

Intercloud Fabric ファイアウォール設定の確認

Intercloud Fabric (ICF) ファイアウォール (VSG) 設定を表示するには、**show running-config** コマンドを使用します。

```
firewall# show running-config
```

```
!Command: show running-config
!Time: Fri Sep 26 15:39:57 2014
```

```
version 5.2(1)VSG2(1)
feature telnet
no feature http-server
```

```
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJS1BCFpNRmQK4na. role network-operator
username admin password 5 $1$CbPcXmpk$131YumYWi00X/EY1qYsFB. role network-admin
username vsnbetauser password 5 $1$mr/jBgON$hoJsM9ACdPHRWPM3KpI6/1 role network-admin
```

```
banner motd #Nexus VSN#
```

```
ssh key rsa 2048
ip domain-lookup
ip domain-lookup
hostname firewall
snmp-server user admin auth md5 0x0b4894684d52823092c7a7c0b87a853d priv
0x0b4894684d52823092c7a7c0b87a853d localizedkey engineID 128:0:0:9:
3:0:0:0:0:0:0
snmp-server user vsnbetauser auth md5 0x272e8099cab7365fd1649d351b953884 priv
0x272e8099cab7365fd1649d351b953884 localizedkey engineID 128:
0:0:9:3:0:0:0:0:0:0
```

```
vrf context management
```

```
ip route 0.0.0.0/0 10.193.72.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc vsg id 1
limit-resource vlan minimum 16 maximum 2049
limit-resource monitor-session minimum 0 maximum 2
limit-resource vrf minimum 16 maximum 8192
limit-resource port-channel minimum 0 maximum 768
limit-resource u4route-mem minimum 32 maximum 32
limit-resource u6route-mem minimum 16 maximum 16
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8
interface mgmt0
  ip address 10.193.73.185/21
interface data0
cli alias name ukickstart copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-kickstart-mzg.VSG1.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
bootflash:dplug
cli alias name uimage copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-mzg.VSG1.1.bin
bootflash:user_bin
line console
boot kickstart bootflash:/ukickstart sup-1
boot system bootflash:/user_bin sup-1
boot kickstart bootflash:/ukickstart sup-2
boot system bootflash:/user_bin sup-2
mgmt-policy TCP permit protocol tcp
  ha-pair id 25
security-profile profile1
  policy p2
security-profile profile2
  policy p1
custom-attribute state "texas"
object-group g1 net.port
  match 1 eq 80
  match 2 eq 443
zone zone1
  condition 1 net.ip-address eq 1.1.1.1
  condition 2 net.port eq 80
  condition 2 net.port eq 80
rule r2
  condition 1 dst.net.ip-address eq 2.2.2.2
  condition 2 src.net.ip-address eq 1.1.1.1
  condition 3 src.net.port eq 100
  condition 4 dst.net.port eq 80
  condition 5 net.protocol eq 6
  action 1 permit
rule r5
  condition 1 net.ethertype eq 0x800
  action 1 inspect ftp
rule r6
rule r7
policy p2
  rule r2 order 10
policy p1
  rule r2 order 10

service firewall logging enable
vnm-policy-agent
  registration-ip 10.193.73.190
  shared-secret *****
  log-level info
firewall#
```




第 3 章

コマンドラインインターフェイスの使用

この章の内容は、次のとおりです。

- [CLI プロンプトの概要, 23 ページ](#)
- [コマンドモード, 24 ページ](#)
- [特殊文字, 24 ページ](#)
- [キーストローク ショートカット, 25 ページ](#)
- [コマンドの省略形, 27 ページ](#)
- [ヘルプの使用, 28 ページ](#)

CLI プロンプトの概要

Intercloud Fabric VSG にアクセスするために、管理 IP に SSH でアクセスします。システムに正常にアクセスした後、リモートワークステーションのターミナルウィンドウに、次のような CLI プロンプトが表示されます。

```
firewall#
```



(注) スイッチの既存のホスト名を表示するには、`show host name` コマンドを使用します。

CLI プロンプトから、次の方法を実行できます。

- 機能を設定するための CLI コマンドを使用する。
- コマンド履歴にアクセスする。
- コマンド解析機能を使用する。

コマンドモード

コマンドモードに関する情報

CLI は、いくつかのコマンドモードに分けられます。ユーザが実行できるアクションは、コマンドモードによって定義されます。コマンドモードは「ネスト」されており、順番にアクセスされます。初めてログインしたときは CLI EXEC モードで開始されます。

EXEC モードからグローバル コンフィギュレーションモードにナビゲートしていくと、使用できるコマンド数が増えます。

コマンドモードの概要

表 5: コマンドモードの概要

モード	アクセス方法	プロンプト	終了方法
EXEC	ログインプロンプトから、ユーザ名とパスワードを入力します。	firewall#	終了してログインプロンプトに戻るには、 exit コマンドを使用します。
ゾーン設定	グローバル コンフィギュレーションモードから、 zonezone-name コマンドを入力します。	firewall (config-zone)#	終了してグローバル コンフィギュレーションモードに戻るには、 exit コマンドを使用します。 終了して EXEC モードに戻るには、 end コマンドを使用するか、Ctrl+Z を押します。
data0 インターフェイス コンフィギュレーション	グローバル コンフィギュレーションモードから interface data0 コマンドを入力します。	firewall (config-if)#	終了してグローバル コンフィギュレーションモードに戻るには、 exit コマンドを使用します。 終了して EXEC モードに戻るには、 end コマンドを使用するか、Ctrl+Z を押します。

特殊文字

次の表に、テキスト文字列で特別な意味を持つ文字を示します。正規表現あるいはその他の特異なコンテキストでのみ使用します。

表 6: 特殊文字

文字	説明
	縦線
<>	より小さい、またはより大きい

キーストローク ショートカット

次の表に、EXEC モードおよびコンフィギュレーションモードの両方で使用されるコマンドキーの組み合わせを示します。

キー	説明
Ctrl+A	カーソルを行の先頭に移動します。
Ctrl+B	カーソルを1文字左に移動します。複数行にわたってコマンドを入力するときは、左矢印キーまたは Ctrl+B キーを繰り返し押し続けてシステムプロンプトまでスクロールバックして、コマンドエントリの先頭まで移動できます。あるいは Ctrl+A キーを押してコマンドエントリの先頭に移動します。
Ctrl+C	コマンドを取り消して、コマンドプロンプトに戻ります。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+E	カーソルを行の末尾に移動します。
Ctrl+F	カーソルを1文字右に移動します。
Ctrl+G	コマンドストリングを削除せずに、コマンドモードを終了して以前のコマンドモードに戻ります。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+L	現在のコマンドラインを再表示します。
Ctrl-R	現在のコマンドラインを再表示します。

キー	説明
Ctrl+T	カーソルの左にある文字を、カーソルの右にある文字と置き換えます。
Ctrl+U	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Ctrl+X、H	履歴を表示します。 このキーの組み合わせを使用するときは、Ctrl キーと X キーを同時に押してリリースしてから、H を押します。
Ctrl+Y	バッファ内の最新のエントリを呼び出します (キーを同時に押します)。
Ctrl-Z	コンフィギュレーションセッションを終了して、EXEC モードに戻ります。 有効なコマンドを入力してから、コマンドラインの最後で Ctrl+Z を使用すると、コマンドの結果の設定がまず実行コンフィギュレーションファイルに追加されます。
↑キー	コマンド履歴の前のコマンドを表示します。
下矢印キー	コマンド履歴の次のコマンドを表示します。
→キーと←キー	コマンド履歴内でカーソルを移動して、コマンドストリングを見つけます。
?	使用可能なコマンドのリストを表示します。

キー	説明
タブ	<p>ワードの最初の文字を入力して Tab キーを押すと、ワードが補完されます。文字に一致するすべてのオプションが表示されます。</p> <p>次の名前を補完する場合に使用します。</p> <ul style="list-style-type: none"> • コマンド名 • ファイル システム内のスキーム名 • ファイル システム内のサーバ名 • ファイル システム内のファイル名 <p>次に、タブのキーストロークを使用する例を示します。</p> <pre>firewall(config)# xm<Tab> firewall(config)# xml <Tab> firewall(config)# xml server</pre> <p>次に、タブのキーストロークを使用する例を示します。</p> <pre>firewall(config)# ns<Tab> nsc-policy-agent vns-binding firewall(config)# security-pr<Tab> firewall(config)# security-profile</pre>

コマンドの省略形

コマンドの最初の数文字を入力することで、コマンドおよびキーワードを省略できます。省略形には、コマンドまたはキーワードを一意に識別でき得る文字数を含める必要があります。コマンドの入力で問題が生じた場合は、システムプロンプトを確認し、疑問符 (?) を入力して使用できるコマンドのリストを表示してください。コマンドモードが間違っているか、間違った構文を使用している可能性があります。

次の表に、コマンド省略形の例を示します。

表 7: コマンド省略形の例

コマンド	省略形
show running-config	sho run

ヘルプの使用

CLI には次のヘルプ機能があります。

表 8: CLI ヘルプ機能

機能	説明
?	有効な入力オプションを一覧表示するには、疑問符 (?) を入力します。
^	CLI はキャレット記号 (^) を構文行の下に出力して、コマンドストリング、キーワード、または引数の入力エラーを示します。
↑キー	↑を使用して、直前に入力したコマンドを CLI に表示し、エラーを修正することができます。

構文エラーの分離および状況依存ヘルプ

次の表は、構文エラーの分離および状況依存ヘルプのコマンドについて説明します。

コマンド	目的
show interface ?	EXEC モードで、 show interface コマンドと一緒に使用されるオプションのパラメータを表示します。
show interface module ?	無効なコマンドエラーのメッセージを表示して、構文エラーをポイント (^) します。
Ctrl-P または上向き矢印	直前に入力したコマンドを表示して、エラーを修正できます。
show interface data ?	データ インターフェイス (data0) を表示するための構文を表示します。
show interface data0	データ インターフェイス (data0) を表示します。

次に、構文エラーの分離および状況依存ヘルプの使用方法を示します。

```
firewall# show interface ?
<CR>
```

```
> Redirect it to a file
>> Redirect it to a file in append mode
brief Show brief info of interface
capabilities Show interface capabilities information
control Data interface
counters Show interface counters
description Show interface description
mac-address Show interface MAC address
mgmt Management interface
module Limit display to interfaces on a specified module
snmp-ifindex Show snmp ifindex list
start Show interfaces starting at a given offset
status Show interface line status
switchport Show interface switchport information
transceiver Show interface transceiver information
trunk Show interface trunk information
| Pipe command output to filter

firewall-1# show interface data0
firewall-1#
firewall#
firewall# show interface data0
data0 is up
  Hardware: Ethernet, address: 0050.5691.53b6 (bia
0050.5691.53b6)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
full-duplex, 1000 Mb/s
Auto-Negotiation is turned on
1 minute input rate 1920 bits/sec, 0 packets/sec
1 minute output rate 24 bits/sec, 0 packets/sec
Rx
  91082 input packets 0 unicast packets 2935 multicast
packets
  88147 broadcast packets 20642956 bytes
Tx
  21968 output packets 0 unicast packets 21968 multicast
packets
  0 broadcast packets 5228289 bytes
firewall#
```




第 4 章

システム管理の設定

この章の内容は、次のとおりです。

- [Intercloud Fabric ファイアウォール設定の確認, 31 ページ](#)
- [ファイルのコピーとバックアップ, 40 ページ](#)
- [ディレクトリの作成, 41 ページ](#)
- [既存のディレクトリの削除, 42 ページ](#)
- [ファイルの移動, 42 ページ](#)
- [ファイルまたはディレクトリの削除, 43 ページ](#)
- [ファイルの圧縮, 44 ページ](#)
- [ファイルの圧縮解除, 45 ページ](#)
- [コマンド出力のファイル保存, 46 ページ](#)
- [ファイルの表示, 46 ページ](#)
- [現在のユーザ アクセスの表示, 48 ページ](#)
- [ユーザへのメッセージ送信, 48 ページ](#)

Intercloud Fabric ファイアウォール設定の確認

Intercloud Fabric (ICF) ファイアウォール (VSG) の設定を確認するには、次のコマンドを入力します。

コマンド	目的
<code>firewall# show version</code>	現在 ICF ファイアウォールで動作しているシステムソフトウェアとハードウェアのバージョンを表示します。

コマンド	目的
firewall# show running-config	現在 ICF ファイアウォールで動作しているシステムソフトウェアとハードウェアのバージョンを表示します。

show version の例

```
firewall# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  kickstart: version 5.2(1)VSG2(1.1)
  system:     version 5.2(1)VSG2(1.1)
  system image file is:  bootflash:///nexus-1000v.5.2.1.VSG2.1.1.bin
  system compile time:   9/25/2014 15:00:00 [09/25/2014 17:43:04]

Hardware
  cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2650 with 4024624 kB of memory.
  Processor Board ID T000200000E

  Device name: firewall-3
  bootflash:   3532446 kB

System uptime is 2 days, 8 hours, 36 minutes, 42 seconds
Kernel uptime is 2 day(s), 8 hour(s), 32 minute(s), 6 second(s)

plugin
  Core Plugin, Ethernet Plugin, Virtualization Plugin
```

show running-config の例

```
firewall# show running-config
!Command: show running-config
!Time: Mon Sep 29 23:03:20 2014

version 5.2(1)VSG2(1.1)
hostname firewall-3

no feature telnet

username admin password 5 $1$74dihjRf$8zkGP9bTIBAwTDOONVsNs. role network-admin
username cmadmin password 5 $1$61wTd4hg$Jjehs1ZhdpvgvZMzqJCf01 role network-admin

banner motd #Nexus Virtual Security Gateway
#

ssh key rsa 2048
no ip domain-lookup
ip host firewall-3 10.37.29.5
no snmp-server protocol enable
snmp-server user admin network-admin auth md5 0xcbb01d04d17237cc045d7b7dd8c33791 priv
0xcbb01d04d17237cc045d7b7dd8c33791 loc
alizedkey
```

```

snmp-server user cmadmin network-admin auth md5 0xb64ad6879970f0e57600c443287a79f0 priv
0xb64ad6879970f0e57600c443287a79f0 1
ocalizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context management
  ip route 0.0.0.0/0 10.37.0.1
port-profile default max-ports 32

system storage-loss log time 30
system inter-sup-heartbeat time 15

interface mgmt0
  ip address 10.37.29.5/16

interface control0
  ip address 40.9.9.31/24
line console
  exec-timeout 5
line vty
  exec-timeout 5
  ha-pair id 0

security-profile default@root
  policy default@root
  custom-attribute vnsporg "root"

security-profile spl@root/T1
  policy ps1@root/T1
  custom-attribute vnsporg "root/t1"
rule acl1/vm_attr@root/T1 cond-match-criteria: match-all
  src-attributes
    condition 10 src.vm.portprofile-name contains 404
  action permit
rule default/default-rule@root cond-match-criteria: match-all
  action drop
Policy default@root
  rule default/default-rule@root order 2
Policy ps1@root/T1
  rule acl1/vm_attr@root/T1 order 101
service firewall logging enable
nsc-policy-agent
  registration-ip 10.36.6.61
  shared-secret *****
  policy-agent-image bootflash:/vnmc-vsgpa.2.0.0.72.bin
  log-level info
logging monitor 6

```

インターフェイス コンフィギュレーションの表示

インターフェイス コンフィギュレーションを表示するには、次のコマンドを入力します。

コマンド	目的
<code>firewall# show interface {type} {name}</code>	特定のインターフェイス接続の詳細を表示します。
<code>firewall# show interface brief</code>	全インターフェイスの概要を表示します。

コマンド	目的
firewall# show running-config interface	システム上の全インターフェイスの実行コンフィギュレーションを表示します。

show interface の例

```
firewall# show interface mgmt 0
mgmt0 is up
Hardware: Ethernet, address: 3a00.0200.000e (bia 3a00.0200.000e)
Internet Address is 10.37.29.5/16
MTU 1352 bytes, BW 1000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
auto-duplex, auto-speed
Auto-Negotiation is turned on
1 minute input rate 1616 bits/sec, 2 packets/sec
1 minute output rate 760 bits/sec, 0 packets/sec
Rx
 477533 input packets 20917 unicast packets 72601 multicast packets
 384015 broadcast packets 37117800 bytes
Tx
 11052 output packets 4253 unicast packets 3404 multicast packets
 3395 broadcast packets 1285641 bytes
```

show interface brief の例

```
firewall# show interface brief

-----
Port      VRF      Status IP Address      Speed  MTU
-----
mgmt0    --      up      10.37.29.3      --     1352
-----

Port      VRF      Status IP Address      Speed  MTU
-----
control0 --      up      41.10.10.20     --     8853
-----

NOTE : * Denotes ports on modules which are currently offline on VSM
firewall#
```

show running-config interface の例

```
firewall# show running-config interface

!Command: show running-config interface
!Time: Mon Sep 29 04:06:33 2014

version 5.2(1)VSG2(1.1)

interface mgmt0
 ip address 10.37.29.3/16

interface control0
 ip address 41.10.10.20/24

firewall#
```

Intercloud Fabric ファイアウォールインスタンスの表示

Intercloud Fabric (ICF) ファイアウォール (VSG) インスタンスを表示できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順の概要

1. vsg# show vsg

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	vsg# show vsg	ICF ファイアウォールモデル、ソフトウェアバージョンとビルド、および Cisco Prime ネットワーク サービス コントローラ (PNSC) IP アドレスを表示します。

次に、ICF ファイアウォール モデル、ソフトウェア バージョンとビルド、および Cisco PNSC IP アドレスを表示する例を示します。

```
vsg# show vsg
Model: VSG
VSG Software Version: 4.2(1)VSG2(1) build [4.2(1)VSG2(1.396)]
PNSC IP: 10.193.20.12
```

ファイル システム内の移動

ファイル システムの指定

ファイル システムを指定するための構文は、<file system name>:[//server/] です。

表 9: ファイル システムの構文の構成要素

ファイル システム名	サーバ	説明
bootflash:	sup-active sup-local sup-1 module-1	アクティブ スーパーバイザにある内部メモリ。システム イメージ、コンフィギュレーション ファイル、およびその他のファイルの格納に使用されます。CLI のデフォルトでは、bootflash: ファイル システムになります。

ファイルシステム名	サーバ	説明
volatile:	—	スーパーバイザ モジュールにある、一時的または保留中の変更のために使用される揮発性 RAM (VRAM)。

現在の作業ディレクトリの特定

CLI 内の現在の場所のディレクトリ名を表示できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順の概要

1. firewall# pwd

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# pwd	CLI 内の現在の場所のディレクトリ名を表示します。

次に、Intercloud Fabric VSG CLI 内の現在の場所のディレクトリ名を表示する例を示します。

```
firewall# pwd
bootflash:
```

ディレクトリの変更

CLI 内のディレクトリを変更できます。

はじめる前に

- 任意のコマンドモードで CLI にログインします。
- Intercloud Fabric (ICF) ファイアウォール (VSG) CLI のデフォルトが、bootflash: ファイルシステムになっていることを確認します。



(注) volatile: ファイルシステムに保存されたファイルは、ICF ファイアウォールのリブート時にすべて消去されます。

手順の概要

1. firewall# **pwd**
2. firewall# **cd** *directory_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# pwd	CLI の現在のディレクトリ名を表示します。
ステップ 2	firewall# cd <i>directory_name</i>	CLI の場所を指定したディレクトリに変更します。

次に、ICF ファイアウォール CLI の現在の場所のディレクトリ名を表示する例と、CLI の場所を、指定したディレクトリに変更する例を示します。

```
firewall# pwd
bootflash:
firewall# cd volatile:
firewall# pwd
volatile:
```

ファイルシステム内のファイルの一覧表示

ディレクトリまたはファイルの内容を表示できます。

はじめる前に

任意のコマンドモードで CLI にログインします。

手順の概要

1. firewall# **dir**[*directory* | *filename*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# dir [<i>directory</i> <i>filename</i>]	ディレクトリまたはファイルの内容を表示します。スラッシュで終わる引数はディレクトリを示し、そのディレクトリの内容が表示されます。

次に、ディレクトリの内容を表示する例を示します。

```
firewall# dir lost+found/
49241 Jul 01 09:30:00 2008 diagclient_log.2613
12861 Jul 01 09:29:34 2008 diagmgr_log.2580
31 Jul 01 09:28:47 2008 dmesg
1811 Jul 01 09:28:58 2008 example_test.2633
89 Jul 01 09:28:58 2008 libdiag.2633
42136 Jul 01 16:34:34 2008 messages
65 Jul 01 09:29:00 2008 otm.log
741 Jul 01 09:29:07 2008 sal.log
87 Jul 01 09:28:50 2008 startupdebug
Usage for log://sup-local
51408896 bytes used
158306304 bytes free
209715200 bytes total
```

ファイルをコピーするために使用できるファイルシステムの特定

ファイルのコピー先またはコピー元になるファイルシステムを特定できます。

はじめる前に

CLI に EXEC モードでログインします。

手順の概要

1. vsg# **copy** ?
2. vsg# **copy filename** ?

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	vsg# copy ?	copy コマンドで使用できるコピー元ファイルシステムを表示します。
ステップ 2	vsg# copy filename ?	copy コマンドで特定のファイルに対して使用できるコピー先ファイルシステムを表示します。

次に、`copy` コマンドで使用できるコピー元ファイルシステムを表示する方法と、指定したファイル名に対する `copy` コマンドで使用できるコピー先ファイルシステムを表示する例を示します。

```
vsg# copy ?
bootflash: Select source filesystem
core: Select source filesystem
debug: Select source filesystem
ftp: Select source filesystem
licenses Backup license files
log: Select source filesystem
nvram: Select source filesystem
running-config Copy running configuration to destination
scp: Select source filesystem
sftp: Select source filesystem
startup-config Copy startup configuration to destination
system: Select source filesystem
tftp: Select source filesystem
volatile: Select source filesystem

vsg# copy filename ?
bootflash: Select destination filesystem
debug: Select destination filesystem
ftp: Select destination filesystem
log: Select destination filesystem
modflash: Select destination filesystem
nvram: Select destination filesystem
running-config Copy from source to running configuration
scp: Select destination filesystem
sftp: Select destination filesystem
startup-config Copy from source to startup configuration
system: Select destination filesystem
tftp: Select destination filesystem
volatile: Select destination filesystem
```

タブ補完の使用

CLI を使用してコマンド内の部分的なファイル名を補完できます。



(注) この手順を使用する前に、EXEC モードで CLI にログインする必要があります。

コマンド	目的
vsg# <code>show file filesystem name: partial filename</code> <TAB>	入力した文字列が単一のファイルに一致する場合、Tab キーを押すとファイル名が補完されます。 一致しない場合は、入力した文字列に一致するファイル名の選択肢の一覧が表示されます。 その後、ファイル名が一意になるために十分な文字数を入力できます。CLI によりファイル名が補完されます。
vsg# <code>show file bootflash:c</code> <TAB>	ファイル名が補完されます。

次に、ファイルまたはファイルのセットが完全に一意になる文字を入力した後 Tab キーを押した場合に使用可能なファイルの選択肢を表示する例を示します。

```
vsg# show file bootflash:nex<Tab>
bootflash:nexus-1000v-dplug-mzg.VSG1.0.1.bin
bootflash:nexus-1000v-kickstart-mzg.VSG1.0.1.bin
bootflash:nexus-1000v-mzg.VSG1.0.1.bin
bootflash:nexus-1000v-mzg.VSG1.0.2.bin
```

次に、コマンドの最初の一意の文字列をすでに入力している場合に、Tab キーを押してコマンドを補完する例を示します。

```
vsg# show file bootflash:c<Tab>
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKbgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQBqogvCPDGeLecA+j
...
...
```

ファイルのコピーとバックアップ

コンフィギュレーションファイルなどのファイルをコピーし、保存するか、または別の場所で再利用することができます。内部ファイルシステムが壊れると、コンフィギュレーションが失われるおそれがあります。コンフィギュレーションファイルは定期的に保存およびバックアップしてください。また、新しいソフトウェアコンフィギュレーションをインストールしたり、新しいソフトウェアコンフィギュレーションに移行する前に、既存のコンフィギュレーションファイルをバックアップしてください。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- 任意のコマンドモードで CLI にログインします。
- 離れた場所にコピーする場合は、デバイスから宛先に到達できるルートがあること。サブネット間でトラフィックをルーティングするルータまたはデフォルトゲートウェイがない場合は、使用デバイスとリモートのコピー先が同じサブネットワーク内にあることが必要です。
- ping コマンドを使用して、デバイスがコピー先に接続できること。
- コピー元のコンフィギュレーションファイルがリモートサーバ上の正しいディレクトリにあること。
- コピー元ファイルのアクセス権が正しく設定されていること。ファイルのアクセス権は、誰でも読み取り可能に設定されている必要があります。



(注) dir コマンドを使用して、コピー先のファイルシステムに十分なスペースがあることを確認してください。十分な領域が残っていない場合は、delete コマンドを使用して不要なファイルを削除します。

手順の概要

1. firewall# **copy** [source filesystem:] filename [destination filesystem:] filename

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# copy [source filesystem:] filename [destination filesystem:] filename	指定したコピー元から指定したコピー先にファイルをコピーします。

次に、指定したコピー元からファイルをコピーし、指定したコピー先に移動する例を示します。

```
firewall# copy system:running-config tftp://10.10.1.1/home/configs/vsg3-run.cfg
Enter vrf (If no input, current vrf 'default' is considered):
Trying to connect to tftp server.....
Connection to Server Established.
TFTP put operation successful
```

ディレクトリの作成

現在のディレクトリ レベルまたは指定したディレクトリ レベルにディレクトリを作成できます。

はじめる前に

この手順を開始する前に、任意のコマンド モードで CLI にログインする必要があります。

手順の概要

1. firewall# **mkdir** {bootflash: | debug: | volatile:} directory-name

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# mkdir {bootflash: debug: volatile:} directory-name	現在のディレクトリ レベルにディレクトリを作成します。

次に、bootflash: ディレクトリに test というディレクトリを作成する例を示します。

```
firewall# mkdir bootflash:test
```

既存のディレクトリの削除

フラッシュ ファイル システムから既存のディレクトリを削除できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- CLI にログインしていること。
- このコマンドは、フラッシュ ファイル システムだけで有効です。
- ディレクトリを削除するには、ディレクトリが空であること。

手順の概要

1. firewall# `rmdir {bootflash: | debug: | volatile:} directory_name`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# <code>rmdir {bootflash: debug: volatile:} directory_name</code>	ディレクトリが空の場合は、削除します。

次に、bootflash: ディレクトリで test というディレクトリを削除する例を示します。

```
firewall# rmdir bootflash:test
```

ファイルの移動

ファイルを別の場所に移動できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- CLI にログインしていること。
- 移動先のディレクトリに十分なスペースがない場合、コピーは完了しないこと。



注意

同じ名前のファイルが移動先のディレクトリに存在する場合、そのファイルは移動するファイルによって上書きされます。

手順の概要

1. firewall# **move** {source_path_and_filename} {destination_path_and_filename}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# move {source_path_and_filename} {destination_path_and_filename}	移動元ディレクトリから移動先ディレクトリにファイルを移動します。

次に、あるディレクトリから同じファイルシステムの別のディレクトリにファイルを移動する例を示します。

```
firewall# move bootflash:samplefile bootflash:mystorage/samplefile
vsg# move samplefile mystorage/samplefile
```

ファイルまたはディレクトリの削除

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- 環境変数 CONFIG_FILE または BOOTLDR で指定されているコンフィギュレーションファイルまたはイメージを削除しようとする、削除を確認するプロンプトが表示されます。
- BOOT 環境変数で指定されている最後の有効なシステムイメージを削除しようとする、削除を確認するプロンプトが表示されます。

手順の概要

1. firewall# **delete** [bootflash: | debug: | log: | volatile:] filename | directory_name

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# delete [bootflash: debug: log: volatile:] filename directory_name	指定したファイルまたはディレクトリ、およびディレクトリ内のすべてを削除します。

次に、現在の作業ディレクトリから指定したファイルを削除し、指定したディレクトリとその内容を削除する例を示します。

```
firewall# delete bootflash:dns_config.cfg
vsg# delete log:my-log
```

ファイルの圧縮

LZ77 コーディングを使用して指定したファイルを圧縮 (zip) できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順の概要

1. firewall# **show command** > [path] filename
2. firewall# **dir**
3. firewall# **gzip** [path] filename

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# show command > [path] filename	show コマンドの出力をファイルに保存します。
ステップ 2	firewall# dir	最初の手順で作成した新しいファイルを含め、現在のディレクトリの内容を表示します。
ステップ 3	firewall# gzip [path] filename	指定したファイルを圧縮します。

次に、指定したファイルを圧縮する例を示します。

```
firewall# show system internal sysmgr event-history errors > errorsfile
firewall# dir
1480264 Nov 03 08:38:21 2001 1
77824 Dec 08 11:17:45 2001 accounting.log
4096 Nov 30 14:35:15 2001 core/
3220 Dec 09 16:33:05 2001 errorsfile
4096 Nov 30 14:35:15 2001 log/
16384 Nov 03 08:32:09 2001 lost+found/
7456 Dec 08 11:17:41 2001 mts.log
1480264 Nov 03 08:33:27 2001 nexus-1000v-dplug-mzg.VSG1.0.1.bin
20126720 Nov 03 08:33:27 2001 nexus-1000v-kickstart-mzg.VSG1.0.1.bin
45985810 Dec 01 14:30:00 2001 nexus-1000v-mzg.VSG1.0.1.bin
46095447 Dec 07 11:32:00 2001 nexus-1000v-mzg.VSG1.0.396.bin
1714 Dec 08 11:17:33 2001 system.cfg.new
4096 Nov 03 08:33:54 2001 vdc_2/
4096 Nov 03 08:33:54 2001 vdc_3/
4096 Nov 03 08:33:54 2001 vdc_4/
Usage for bootflash://
631246848 bytes used
5772722176 bytes free
6403969024 bytes total
```

```

firewall# gzip bootflash:errorsfile
firewall# dir
1480264 Nov 03 08:38:21 2001 1
77824 Dec 08 11:17:45 2001 accounting.log
4096 Nov 30 14:35:15 2001 core/
861 Dec 09 16:33:05 2001 errorsfile.gz
4096 Nov 30 14:35:15 2001 log/
16384 Nov 03 08:32:09 2001 lost+found/
7456 Dec 08 11:17:41 2001 mts.log
1480264 Nov 03 08:33:27 2001 nexus-1000v-dplug-mzg.VSG1.0.1.bin
20126720 Nov 03 08:33:27 2001 nexus-1000v-kickstart-mzg.VSG1.0.1.bin
45985810 Dec 01 14:30:00 2001 nexus-1000v-mzg.VSG1.0.1.bin
46095447 Dec 07 11:32:00 2001 nexus-1000v-mzg.VSG1.0.396.bin
1714 Dec 08 11:17:33 2001 system.cfg.new
4096 Nov 03 08:33:54 2001 vdc_2/
4096 Nov 03 08:33:54 2001 vdc_3/
4096 Nov 03 08:33:54 2001 vdc_4/
Usage for bootflash://
631246848 bytes used
5772722176 bytes free
6403969024 bytes total

```

ファイルの圧縮解除

LZ77 コーディングを使用して、圧縮済みの指定したファイルを圧縮解除 (unzip) できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順の概要

1. firewall# **gunzip** *[path] filename*
2. firewall# **dir**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# gunzip <i>[path] filename</i>	指定したファイルを圧縮解除します。
ステップ 2	firewall# dir	新たに圧縮解除したファイルを含め、ディレクトリの内容を表示します。

次に、指定したファイルを圧縮解除する例を示します。

```

firewall# gunzip bootflash:errorsfile.gz
firewall# dir bootflash:
1480264 Nov 03 08:38:21 2001 1
77824 Dec 08 11:17:45 2001 accounting.log
4096 Nov 30 14:35:15 2001 core/
3220 Dec 09 16:33:05 2001 errorsfile
4096 Nov 30 14:35:15 2001 log/
16384 Nov 03 08:32:09 2001 lost+found/
7456 Dec 08 11:17:41 2001 mts.log

```

```

1480264 Nov 03 08:33:27 2001 nexus-1000v-dplug-mzg.VSG1.0.1.bin
20126720 Nov 03 08:33:27 2001 nexus-1000v-kickstart-mzg.VSG1.0.1.bin
45985810 Dec 01 14:30:00 2001 nexus-1000v-mzg.VSG1.0.1.bin
46095447 Dec 07 11:32:00 2001 nexus-1000v-mzg.VSG1.0.396.bin
1714 Dec 08 11:17:33 2001 system.cfg.new
4096 Nov 03 08:33:54 2001 vdc_2/
4096 Nov 03 08:33:54 2001 vdc_3/
4096 Nov 03 08:33:54 2001 vdc_4/
Usage for bootflash://sup-local
631246848 bytes used
5772722176 bytes free
6403969024 bytes total

```

コマンド出力のファイル保存

コマンド出力をファイルに保存できます。

はじめる前に

この手順を開始する前に、任意のコマンドモードで CLI にログインする必要があります。

手順の概要

1. firewall# **show running-config** > [*path* | *filename*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# show running-config > [<i>path</i> <i>filename</i>]	コマンド出力を、指定したパスおよびファイル名に保存します。

次に、コマンド出力を volatile: ディレクトリのファイル vsg1-run.cfg に保存する例を示します。

```
firewall# show running-config > volatile:vsg1-run.cfg
```

ファイルの表示

ファイルに関する情報を表示するには、次のコマンドを入力します。

コマンド	目的
firewall# show file [bootflash: debug: volatile:] <i>filename</i>	指定されたファイルの内容を表示します。
firewall# pwd	現在の作業ディレクトリを表示します。
firewall# dir	ディレクトリの内容を表示します。

コマンド	目的
<code>firewall# show file filename [cksum md5sum]</code>	ファイルのチェックサムまたは Message Digest アルゴリズム5 (MD5) チェックサムを指定し、元のファイルと比較します。MD5 はファイルの電子的なフィンガープリントです。
<code>firewall# tail {path}[filename] {number-of-lines}</code>	指定したファイルの末尾から、要求された数の行を表示します。 number-of-lines 引数の範囲は 0 ~ 80 です。
<code>firewall# show users</code>	Intercloud Fabric ファイアウォールに現在アクセスしているユーザのリストを表示します。

show file の例

```
firewall# show file bootflash:sample_file.txt
security-profile sp1
policy p1
rule r1
action 10 permit
policy p1
rule r1 order 10
```

dir コマンドの例

```
firewall# dir
Usage for volatile://
0 bytes used
20971520 bytes free
20971520 bytes total
```

show file cksum コマンドの例

```
firewall# show file bootflash:sample_file.txt cksum
750206909
```

show file md5sum コマンドの例

```
firewall# show file bootflash:sample_file.txt md5sum
aa163ec1769b9156614c643c926023cf
```

tail コマンドの例

```
firewall# tail bootflash:errorsfile 5
(20) Event:E_DEBUG, length:34, at 171590 usecs after Tue Jul 1 09:29:05 2014
[102] main(326): stateless restart
```

tail コマンドの例

```
firewall# show users
NAME LINE TIME IDLE PID COMMENT
admin pts/0 Jul 1 04:40 03:29 2915 (::ffff:64.103.145.136)
admin pts/2 Jul 1 10:06 03:37 6413 (::ffff:64.103.145.136)
admin pts/3 Jul 1 13:49 . 8835 (171.71.55.196)*
```

現在のユーザ アクセスの表示

Intercloud Fabric VSG に現在アクセスしているすべてのユーザを表示できます。

はじめる前に

CLI に EXEC モードでログインします。

手順の概要

1. firewall# **show user**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# show user	Intercloud Fabric VSG に現在アクセスしているユーザのリストを表示します。

次に、Intercloud Fabric VSG に現在アクセスしているユーザのリストを表示する例を示します。

```
firewall# show users
NAME LINE TIME IDLE PID COMMENT
admin pts/0 Jul 1 04:40 03:29 2915 (::ffff:64.103.145.136)
admin pts/2 Jul 1 10:06 03:37 6413 (::ffff:64.103.145.136)
admin pts/3 Jul 1 13:49 . 8835 (171.71.55.196) *
```

ユーザへのメッセージ送信

Cisco VSG を現在使用しているすべてのアクティブ ユーザにメッセージを送信できます。

はじめる前に

この手順を開始する前に、CLI にログインする必要があります。

手順の概要

1. firewall# **send {session device} line**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	firewall# send { <i>session device</i> } <i>line</i>	現在システムにログインしているユーザにメッセージを送信します。 次のキーワードと引数を使用できます。 <ul style="list-style-type: none">• session : 指定された pts または tty デバイス タイプにメッセージを送信します。• line は最大 80 文字の英数字からなるメッセージです。

次に、すべてのユーザにメッセージを送信する例を示します。

```
firewall# send Hello. Shutting down the system in 10 minutes.  
Broadcast Message from admin@vsg (/dev/pts/34) at 8:58 ...  
Hello. Shutting down the system in 10 minutes.
```




第 5 章

SNMP の設定

この章の内容は、次のとおりです。

- [SNMP に関する情報, 51 ページ](#)
- [注意事項と制約事項, 55 ページ](#)
- [SNMP の設定, 55 ページ](#)
- [SNMP の設定確認, 56 ページ](#)
- [MIB, 57 ページ](#)

SNMP に関する情報

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージフォーマットを提供します。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- **SNMP マネージャ**：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- **SNMP エージェント**：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。Intercloud Fabric ファイアウォール (VSG) は、エージェントおよび MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。
- **管理情報ベース (MIB)**：SNMP エージェント上の管理対象オブジェクトのコレクション。
- SNMP は、RFC 3411 ~ 3418 で規定されています。



(注) SNMP ロールベース アクセス コントロール (RBAC) はサポートされていません。SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知によって、不正なユーザ認証、再起動、接続の終了、ネイバールータとの接続切断、またはその他の重要イベントを示すことができます。

SNMP 通知は、トラップまたは応答要求として生成されます。トラップは、エージェントからホストレシーバテーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。応答要求は、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても Acknowledgment (ACK; 確認応答) を送信しないからです。Intercloud Fabric ファイアウォール (VSG) は、トラップが受信されたかどうかを判断することはできません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答 Protocol Data Unit (PDU; プロトコルデータユニット) でメッセージの受信を確認します。ICF ファイアウォールが応答を受信しない場合、インフォーム要求を再度送信できます。ICF ファイアウォールを複数のホストレシーバに通知を送信するように設定できます。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュアアクセスを実現します。SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：有効な送信元からのメッセージであるかどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティモデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティレベルとは、セキュリティモデル内で許可されるセキュリティのレベルです。セキュリティモデルとセキュリティレベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティメカニズムが決まります。

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル。
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv：認証と暗号化両方を実行するセキュリティ レベル。

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

表 10: SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	No	コミュニティ ストリングの照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code (HMAC) メッセージダイジェスト 5 (MD5) アルゴリズムまたは HMAC Secure Hash Algorithm (SHA) アルゴリズムに基づく認証はされません。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格 (DES) の 56 ビット暗号化、および暗号ブロック連鎖 (CBC) DES (DES-56) 標準に基づいた認証を提供します。

ユーザベースのセキュリティ モデル

SNMPv3 ユーザベース セキュリティ モデル (USM) は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データシーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。Cisco VSG は SNMPv3 に 2 種類の認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco VSG は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard (AES) を使用します。AES は RFC 3826 に準拠しています。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES を選択できます。priv オプションを aes-128 トークンと併用すると、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合は、大文字と小文字を区別して、最大 64 文字の英数字を指定できます。ローカライズしたキーを使用する場合は最大 130 文字の英数字を指定できます。外部 AAA (認証、許可、アカウントिंग) サーバを使用する SNMPv3 動作の場合は、外部 AAA サーバ上のユーザ コンフィギュレーションで、プライバシー プロトコルとして AES を使用する必要があります。

コマンドライン インターフェイス (CLI) および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting (AAA) サーバ レベルで集中化できます。この集中型ユーザ管理により、Intercloud Fabric (ICF) ファイアウォール (VSG) の SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証された後、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザグループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

ICF ファイアウォールはユーザ設定を次の方法で同期します。

- `snmp-server user` コマンドで指定された認証パスフレーズが CLI ユーザのパスワードになります。
- `username` コマンドで指定されたパスワードが SNMP ユーザの認証およびプライバシー パスフレーズになります。

- SNMP または CLI を使用してユーザを削除すると、SNMP と CLI の両方でユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- CLI から行ったロール変更（削除または変更）は、SNMP と同期します。



(注) ローカライズしたキー/暗号化形式でパスフレーズ/パスワードを設定すると、ICF ファイアウォールはパスワードを同期しません。

Cisco NX-OS ソフトウェアはデフォルトで、同期したユーザ設定を 60 分間維持します。

グループベースの SNMP アクセス



(注) グループとは業界全体で使用される標準的な SNMP 用語であるため、このマニュアルでは、この SNMP の章でグループとしてのロールについて言及します。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは読み取り専用アクセス権または読み取り/書き込みアクセス権を指定して定義します。ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

注意事項と制約事項

SNMP には、次の注意事項および制限事項があります。

- 一部の SNMP MIB に対する読み取り専用アクセスがサポートされています。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポート リストを参照してください。
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>
- SNMP ロールベース アクセス コントロール (RBAC) はサポートされていません。
- SNMP 設定コマンドは、次の Cisco MIB でサポートされています。
 - CISCO-IMAGE-UPGRADE-MIB
 - CISCO-CONFIG-COPY-MIB

SNMP の設定

SNMP の設定については、『Cisco Prime Network Services Controller GUI Configuration Guide』を参照してください。

SNMP の設定確認

SNMP の設定を表示するには、次のいずれかのコマンドを使用します。

表 11 : *SNMP* 設定の確認コマンド

コマンド	目的
show running-config snmp [all]	SNMP の実行コンフィギュレーションを表示します。
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティストリングを表示します。
show snmp context	SNMP コンテキストマッピングを表示します。
show snmp engineID	SNMP エンジン ID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp session	SNMP セッションを表示します。
show snmp trap	SNMP の有効通知または無効通知を表示します。
show snmp user	SNMP ユーザを表示します。

MIB

表 12 : サポート対象 MIB

MIB	MIB リンク
	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MIB	MIB リンク
<ul style="list-style-type: none"> • CISCO-TC • SNMPv2-MIB • SNMP-FRAMEWORK-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • ENTITY-MIB • CISCO-ENTITY-EXT-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-VIRTUAL-NIC-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB • NOTIFICATION-LOG-MIB • IANA-ADDRESS-FAMILY-NUMBERS-MIB • IANAifType-MIB • IANAiprouteprotocol-MIB • HCNUM-TC • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-SYSTEM-MIB • CISCO-SYSTEM-EXT-MIB • ISCO-IMAGE-MIB • CISCO-IMAGE-UPGRADE-MIB • CISCO-BRIDGE-MIB • CISCO-CONFIG-COPY-MIB • CISCO-SYSLOG-EXT-MIB • CISCO-PROCESS-MIB • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB • CISCO-COMMON-ROLES-MIB • CISCO-COMMON-MGMT-MIB • CISCO-UNIFIED-FIREWALL-MIB 	



索引

A

ACL [8](#)
AES [53](#)
authNoPriv [53](#)

C

capability l3-vservice [7](#)
Cisco Nexus 1000V シリーズ スイッチ [1](#)
CISCO-CONFIG-COPY-MIB [55](#)
CISCO-IMAGE-UPGRADE-MIB [55](#)
Cisco NX-OS [1](#)
Cisco Prime Network Services Controller [13](#)
Cisco VSG [1,7](#)
 概要 [7](#)
 レイヤ3 モード [7](#)
cli [28](#)
 構文エラーの分離 [28](#)
 状況依存ヘルプ [28](#)
 ヘルプ機能 [28](#)
CLI [23,24](#)
 コマンド モード [24](#)
 prompt [23](#)
copy [38](#)
copy コマンド [40](#)

D

debug [10](#)
DES [53](#)
dir [37](#)

G

gunzip [45](#)

H

HMAC-MD5-96 [53](#)
HMAC-SHA-96 [53](#)

I

ICF ファイアウォール [1](#)
ICF ファイアウォール [7](#)
 導入シナリオ [7](#)
Intercloud Fabric ファイアウォール} [8](#)
 IP アドレス [8](#)
IP アドレス [8,9,14](#)
 VSG [8](#)

M

MIB [51,57](#)
mkdir [41](#)

N

noAuthNoPriv [53](#)
NX-OS [1](#)

P

permit [10](#)
Prime NSC [13](#)
pwd [36](#)

Q

QoS [8](#)

R

rmdir 42

S

show file 46
 show interface 33
 show running-config snmp 56
 show running config 33
 show running configuration 31, 46
 show snmp 56
 show snmp community 56
 show snmp context 56
 show snmp engineID 56
 show snmp group 56
 show snmp session 56
 show snmp trap 56
 show snmp user 56
 show user 48
 show users 46
 show version 31
 show vsg 34
 SNMP 51, 55
 SNMPv1 53
 SNMPv2 53
 SNMPv3 52, 53
 SNMPv3 暗号化 52
 SNMPv3 認証 52
 SNMPv3 ユーザベースのセキュリティ モデル 53
 snmp アクセス 55
 snmp エージェント 51, 52
 snmp 通知 52
 SNMP の制限事項 55
 SNMP の設定 55
 SNMP のユーザ同期 54
 snmp マネージャ 51

T

tail 46

V

vApp 6
 vCenter 9, 14
 VEM 3, 4, 7
 VEM インターフェイス 7
 vEthernet 8

Virtual Security Gateway 1
 ICF ファイアウォールを参照 1
 VLAN 6, 14
 管理 14
 VM 1, 7, 8
 VM モビリティ 7
 セグメンテーション 8
 ポートプロファイル 8
 VM ポートプロファイル 10
 vNIC 3
 VNMC IP アドレスの表示 34
 volatile 35
 vPath 3, 7, 8
 vservice 7
 VSM 8

あ

アクション 10
 permit 10
 インспекション 10
 ドロップ パケット 10
 ログ 10
 アクセス コントロール ルール 6
 アクセス ログ 6
 アクティブ/スタンバイ ペア 6
 アクティブ/スタンバイ モード 3

い

イーサネット 8
 move 42
 インспекション 10
 interface 8
 管理 8

お

オブジェクトグループ 9, 15
 例 15
 オペレーション分離 3

か

解凍 45

カスタム属性 [8, 10, 17, 19](#)
 仮想イーサネット ポート [6](#)
 Virtual Ethernet Module (仮想イーサネット モジュール) [3](#)
 VEM を参照 [3](#)
 仮想インフラストラクチャ属性 [17](#)
 仮想化 [6](#)
 仮想化データセンター [7](#)
 仮想サービス ノード [7](#)
 仮想スイッチ [6](#)
 仮想スーパーバイザ モジュール [6](#)
 仮想データセンター [1, 6](#)
 仮想ネットワーク サービス データパス [3](#)
 仮想ファイアウォール [1](#)
 仮想ポート [8](#)
 仮想マシン [1](#)
 VM を参照 [1](#)
 環境 [6](#)
 VM [6](#)
 処理のために [6](#)
 管理インターフェイス [8](#)
 administrator [8, 9](#)
 ネットワーク [8](#)
 security [8, 9](#)

き

キーボードショートカット [25](#)
 キャパシティ プランニング [3](#)

く

クラウド VSG [2](#)
 設定 [2](#)
 クラウド環境 [1](#)
 グループベースの SNMP アクセス [55](#)

け

現在のディレクトリ [36](#)
 現在のユーザのリスト [48](#)

こ

構造化環境 [6](#)

高速パス モード [4](#)
 構文エラーの分離 [28](#)
 command [24](#)
 特殊文字 [24](#)
 コマンド: 省略形 [27](#)
 コマンド: ヘルプ機能 [28](#)
 コマンド出力のファイル保存 [46](#)
 コマンドショートカット [25](#)
 コマンドモード [24](#)
 コンピュータ インフラストラクチャ [1](#)

さ

サービス ファイアウォール ログ [10](#)
 delete [43](#)
 サブネット [9, 14](#)

し

コンプライアンス [1](#)
 状況依存ヘルプ [28](#)
 使用できるファイル システムの特定 [38](#)
 信頼ゾーン [1, 6](#)
 定義 [6](#)

す

スタンバイ VSG [3](#)

せ

セキュリティ運用 [3](#)
 セキュリティ管理者 [8](#)
 セキュリティ サービス [8](#)
 セキュリティ プロファイル [6, 8, 19](#)
 セキュリティ プロファイル テンプレート [1](#)
 セキュリティ ポリシー [1](#)
 セキュリティ モデル [53](#)
 セグメンテーション [8](#)
 VM [8](#)
 session [48](#)
 設定時の注意事項および制限事項 [14](#)
 設定の表示 [20](#)
 専用サーバ [3](#)

そ

send [48](#)
 zone [6, 9, 14, 19](#)
 属性 [19](#)
 membership [6](#)
 例 [14](#)
 ゾーンからゾーンへのトラフィック [6](#)
 ゾーン属性 [9, 14](#)
 ゾーンメンバーシップ [6](#)
 属性 [6, 8, 9, 14, 16, 17, 19](#)
 port-profile [17](#)
 custom [8, 17, 19](#)
 仮想インフラストラクチャ [17](#)
 classes [17](#)
 指向性 [16](#)
 ニュートラル [9, 14, 17](#)
 ソフトスイッチ [8](#)

た

timeout [4](#)
 高速パスモード [4](#)

て

ディレクトリ内のファイルの一覧表示 [37](#)
 ディレクトリの削除 [42, 43](#)
 ディレクトリの作成 [41](#)
 データインターフェイス [14](#)
 テナントトラフィック [8](#)
 展開設定 [2](#)

と

同期 [54](#)
 導入 [7](#)
 トラップ [52](#)
 トラフィック [6](#)
 外部からゾーン [6](#)
 ゾーンから外部 [6](#)
 ゾーンからゾーン [6](#)
 ポリシーベース [6](#)
 ドロップパケット [10](#)

に

ニュートラル属性 [9, 14, 17](#)
 認証プロトコル [53](#)

ね

ネットワーク管理者 [8](#)

は

ハイアベイラビリティ [3](#)
 ハイパーバイザ [3](#)
 passphrase [54](#)
 バックアップファイル [40](#)

ふ

ファイアウォール [20](#)
 ロギング [20](#)
 ファイアウォール設定の確認 [31](#)
 ファイアウォールの表示 [34](#)
 ファイアウォールポリシー [10, 16, 19](#)
 例 [16](#)
 ファイアウォールポリシーオブジェクト [13](#)
 設定の要件 [13](#)
 ファイアウォールルール [9, 10, 15](#)
 file system [35](#)
 ファイルの圧縮解除 [45](#)
 ファイルの移動 [42](#)
 ファイルのコピー [40](#)
 ファイルの削除 [43](#)
 ファイルの表示 [46](#)
 ファイル名のコピー [38](#)
 ブートフラッシュ [35](#)
 プライマリ VSG [3](#)

ほ

方向属性 [16](#)
 ポートグループ [8](#)
 ポートプロファイル [6, 8, 10, 19](#)
 VM [8](#)
 ポートプロファイル属性 [17](#)
 ホスト [9, 14](#)

ポリシー 8

ACL 8

QoS 8

ポリシー オブジェクト 10, 16

condition 16

アクション 16

オブジェクト グループ 16

zone 16

rule 16

ポリシー決定 3

ポリシーの適用 3

ポリシー評価 10

policy name 9, 16

ま

マルチテナント アクセス 7

め

メッセージ整合性 52, 53

メッセージの機密性 53

メッセージ発信元の認証 53

ゆ

ユーザへのメッセージの送信 48

る

ルール 10, 15

例 15

rule 14

ルール条件 9, 15

れ

レイヤ 3 の設定 10

レイヤ 3 モード 7, 10

capability l3-vservice 7

VEM インターフェイス 7

設定 10

ろ

ロール ベース アクセス コントロール 51

ロールベース アクセス コントロール 55

ログ 10

