



INDEX

記号

* (アスタリスク)

自動学習済みエントリ [9-7](#)

ポートセキュリティ ワイルドカード [9-5](#)

数字

3DES 暗号化

IKE [7-7](#)

IPsec [7-6](#)

A

AAA

CFS での配信 (手順) [4-29](#)

アカウントिंग サービスの設定 [4-15 ~ ??](#)

サーバへの配信のイネーブル化 [4-27](#)

説明 [4-1](#)

デフォルト設定 [4-16](#)

認証の設定 [4-14](#)

配信セッションの開始 [4-13](#)

リモート サービス [4-4](#)

ローカル サービス [4-14](#)

AAA サーバ

グループ [4-4](#)

モニタリング [4-5](#)

リモート認証 [4-15](#)

Advanced Encrypted Standard 暗号化。「AES 暗号化」を参照

AES-XCBC-MAC

IPsec [7-6](#)

AES 暗号化

IKE [7-7](#)

IPsec [7-6](#)

AES を使用する Message Authentication Code。「AES-XCBC-MAC」を参照

C

CA

アイデンティティ [6-2](#)

カットアンドペースによる登録 [6-4](#)

最大限度 [6-6](#)

証明書のダウンロード例 [6-18](#)

設定 [6-6 ~ 6-16](#)

設定例 [6-21](#)

デジタル証明書の削除 [6-15](#)

デフォルト設定 [6-6](#)

トラスト ポイントの作成 [6-8](#)

認証 [6-9](#)

ピア証明書 [6-5](#)

複数 [6-5](#)

複数のトラスト ポイント [6-4](#)

メンテナンス [6-13](#)

目的 [6-2](#)

モニタリング [6-13](#)

Certificate Revocation List。「CRL」を参照

Cisco Access Control Server。「Cisco ACS」を参照

Cisco ACS

RADIUS に対する設定 [4-30 ~ 4-34](#)

TACACS+ に対する設定 [4-30 ~ 4-34](#)

cisco-av-pair

SNMPv3 への指定 [4-10](#)

CRL

インポート例 [6-21](#)

失効チェック方式の設定 [6-10](#)
 生成例 [6-20](#)
 設定 [6-15](#)
 説明 [6-5](#)
 ダウンロード例 [6-20](#)

D

Data Encryption Standard 暗号化。「DES 暗号化」を参照

DES 暗号化

IKE [7-7](#)

IPsec [7-6](#)

DH

IKE [7-7](#)

DHCHAP

イネーブル化 [8-3, 8-6](#)

グループ設定 [8-4](#)

設定 [8-6 ~ ??](#)

説明 [8-2](#)

タイムアウト値 [8-5](#)

他の SAN-OS 機能との互換性 [8-3](#)

デフォルト設定 [8-6](#)

認証モード [8-3](#)

ハッシュアルゴリズム [8-4](#)

ライセンス [8-2](#)

リモートデバイスのパスワード [8-5](#)

ローカルスイッチのパスワード [8-4](#)

「FC-SP」も参照 [8-1](#)

Diffie-Hellman Challenge Handshake Authentication Protocol。「DHCHAP」を参照

Diffie-Hellman プロトコル。「DH」を参照

Digital Signature Algorithm。「DSA キー ペア」を参照

DSA キー ペア

生成 [3-14](#)

E

EFMD

ファブリック バインディング [10-1](#)

Exchange Fabric Membership Data。「EFMD」を参照 [10-1](#)

E ポート

ファブリック バインディング チェック [10-2](#)

F

FCIP

DHCHAP との互換性 [8-3](#)

FC-SP

ISL 上でのイネーブル化 [8-5](#)

イネーブル化 [8-6](#)

認証 [8-1](#)

「DHCHAP」も参照 [8-1](#)

Fibre Channel Security Protocol。「FC-SP」を参照

FIPS [2-1](#)

I

ICMP パケット

タイプの値 [5-4](#)

ID

シスコのベンダー ID [4-9](#)

IKE

SA のリフレッシュ [7-27](#)

暗号化トランスフォーム [7-6](#)

初期化 [7-10](#)

設定の表示 (手順) [7-24](#)

説明 [7-4](#)

デフォルト設定 [6-6, 7-22](#)

認証アルゴリズム [7-6](#)

用語 [7-5](#)

IKE ドメイン

クリア [7-27](#)

説明 [7-10](#)

IKE トンネル

クリア [7-27](#)

説明 [7-10](#)

IKE 発信側

バージョンの設定 [7-27](#)

IKE ピア

 キープアライブ タイムの設定 [7-26](#)

IKE ポリシー

 ネゴシエーション [7-10](#)

 ネゴシエーション パラメータの設定 [7-26](#)

IPsec

 FCIP Wizard でのイネーブル化 (手順) [7-23](#)

 RFC 実装 [7-1](#)

 暗号化トランスフォーム [7-6](#)

 クリプト IPv4-ACL [7-12 ~ 7-28](#)

 グローバル ライフタイム値 [7-19](#)

 サポートされていない機能 [7-4](#)

 設定の表示 (手順) [7-24](#)

 デジタル証明書のサポート [7-7 ~ 7-10](#)

 デフォルト設定 [7-22](#)

 トランスフォーム セット [7-15](#)

 認証アルゴリズム [7-6](#)

 ハードウェアの互換性 [7-4](#)

 ファブリック設定の要件 [7-4](#)

 メンテナンス [7-19](#)

 用語 [7-5](#)

 ライセンスの要件 [7-20](#)

IPv4-ACL

 IP-ACL Wizard を使用した作成 (手順) [5-6](#)

 インターフェイスへの適用 [5-9, 5-10](#)

 エントリの削除 [5-8](#)

 エントリの追加 [5-7](#)

 クリプト [7-12 ~ 7-28](#)

 クリプト マップ エントリ [7-16](#)

 設定に関する考慮事項 [5-5](#)

 設定例 [5-11](#)

 ダンプ ログの読み取り [5-9](#)

 複雑な IPv4-ACL の作成 (手順) [5-7](#)

IP セキュリティ。「IPsec」を参照

IP ドメイン名

 デジタル証明書の設定 [6-7](#)

IP フィルタ

 IP-ACL Wizard の使用方法 (手順) [5-6](#)

IP トラフィックの制限 [5-1, 5-2](#)

内容 [5-2](#)

M

MD5 認証

 IKE [7-7](#)

 IPsec [7-6](#)

Message Digest 5。「MD5 認証」を参照

mgmt0 インターフェイス

 デフォルト設定 [3-7, 4-16, 6-6, 7-22, 8-6, 9-10, 10-3](#)

Microsoft Challenge Handshake Authentication Protocol (マイクロソフト チャレンジ ハンドシェイク 認証プロトコル)。「MSCHAP」を参照

MSCHAP

 説明 [4-14](#)

O

Online Certificate Status Protocol。「OCSP」を参照

OSCP

 サポート [6-5](#)

P

PKI

 登録サポート [6-4](#)

R

RADIUS

 AAA プロトコル [4-1](#)

 CFS マージの注意事項 [4-15](#)

 Cisco ACS の設定 [4-30 ~ 4-34](#)

 事前共有キーの設定 [4-8](#)

 設定配信セッションの消去 [4-29](#)

 設定配信のイネーブル化 [4-27](#)

 設定配信の変更の廃棄 [4-29](#)

- 説明 4-17
- タイムアウトの指定 4-19
- テスト アイドル タイマーの設定 4-8
- テスト ユーザ名の設定 4-9
- デフォルト設定 4-16
- 配信セッションの開始 4-13

RSA キー ペア

- インポート 6-6, 6-13
- エクスポート 6-6, 6-13
- 削除 6-16
- 生成 3-14, 6-7
- 説明 6-3
- 複数 6-5

S

SA

- IPSec ピア間での確立 7-17
- ライフタイム ネゴシエーション 7-17
- ライフタイムの設定 7-29
- リフレッシュ 7-27

Secure Hash Algorithm。「SHA-1」を参照

SHA-1

- IKE 7-7
- IPsec 7-6

SNMP

- CLI オペレーションをマッピング 3-5
- セキュリティ機能 4-3
- ロールの作成 3-4

SNMPv3

- cisco-av-pair の指定 4-10

SSH

- イネーブル化 3-16
- サーバ キー ペアの上書き 3-15
- サーバ キー ペアの生成 3-14
- 説明 3-6
- デジタル証明書認証 3-6
- デフォルト サービス 3-14
- ログイン 4-5

SSH キー ペア

- 上書き 3-15

T

TACACS+

- AAA プロトコル 4-1
- CFS マージの注意事項 4-15
- Cisco ACS の設定 4-30 ~ 4-34
- グローバル キー 4-11
- 検証 4-12
- サーバ統計情報の表示 4-35
- 事前共有キーの設定 4-11
- 設定配信セッションの消去 4-29
- 設定配信のイネーブル化 4-27
- 設定配信の変更の廃棄 4-29
- 説明 4-11
- デフォルト設定 4-16
- デフォルトのサーバ タイムアウトの設定 4-24
- デフォルトのサーバの暗号の設定 4-23
- 配信セッションの開始 4-13
- ログイン時にサーバを指定 4-13

TCP ポート

- IPv4-ACL 5-3

Telnet

- イネーブル化 3-16
- ログイン 4-5

TE ポート

- ファブリック バインディング チェック 10-2

Triple DES。「3DEC 暗号化」を参照

TrustSec FC リンク暗号化 11-1

- ESP ウィザード 11-5
- ESP の設定 11-4
- イネーブル化 11-3
- サポートされているモジュール 11-1
- セキュリティ アソシエーション 11-3
- セキュリティ アソシエーション パラメータ 11-3
- 用語 11-2

U

UDP ポート

IPv4-ACL [5-3](#)

V

VSA

属性の通信 [4-9](#)

プロトコル オプション [4-9](#)

VSAN

DHCHAP との互換性 [8-3](#)

IP ルーティング [5-1, 5-2](#)

ルールと機能 [3-2](#)

VSAN ポリシー

デフォルト ロール [3-8](#)

W

WWN

ポート セキュリティ [9-5](#)

あ

アカウントティング

サービスの設定 [4-15](#)

アクセス コントロール リスト。「IPv4-ACL」、
「IPv6-ACL」を参照

い

インターネット キー交換。「IKE」を参照

インターフェイス

デフォルト設定 [3-7, 4-16, 6-6, 7-22, 8-6, 9-10, 10-3](#)

か

管理インターフェイス

デフォルト設定 [3-7, 4-16, 6-6, 7-22, 8-6, 9-10, 10-3](#)

き

共通のユーザ

CLI から SNMP にマッピング [3-5](#)

共通ロール

削除 (手順) [3-9](#)

設定 [3-4](#)

許可

ルール適用順序 [3-10](#)

く

クリプト IPv4-ACL

any キーワード [7-14](#)

設定に関する考慮事項 [7-20](#)

ミラー イメージ [7-13](#)

クリプト マップ

auto-peer オプション [7-18](#)

IPv4-ACL のエントリ [7-16](#)

PFS (完全転送秘密) [7-18](#)

PFS の設定 [7-30](#)

SA ライフタイム ネゴシエーション [7-17](#)

設定に関する考慮事項 [7-22](#)

ピア間の SA [7-17](#)

クリプト マップ エントリ

SA ライフタイムの設定 [7-29](#)

グローバル ライフタイム値 [7-19](#)

クリプト マップ セット

インターフェイスへの適用 [7-19](#)

グローバル キー

RADIUS への割り当て [4-8](#)

こ

公開キー インフラストラクチャ。「PKI」を参照

し

シスコのベンダー ID

説明 4-9

事前共有キー

RADIUS 4-8

TACACS+ 4-11

す

スイッチ セキュリティ

デフォルト設定 3-7, 4-16

せ

セキュリティ

アカウントینگ 4-4

スイッチ上での管理 4-1

セキュリティ アソシエーション。「SA」を参照

セキュリティ制御

リモート 4-2, 4-17

リモート AAA サーバ 4-16

ローカル 4-2

て

デジタル証明書

CA からの削除 6-15

IPsec 7-7 ~ 7-10

SSH サポート 3-6

アイデンティティ証明書のインストール 6-11

アイデンティティ証明書の要求例 6-19

アイデンティティ証明書要求の生成 6-11

インポート 6-6, 6-13

エクスポート 6-6, 6-13

最大限度 6-6

失効例 6-20

設定 6-6 ~ 6-16

設定例 6-16 ~ 6-18

デフォルト設定 6-6

ピア 6-5

メンテナンス 6-13

目的 6-2

モニタリング 6-13

と

トラスト ポイント

作成 6-8

説明 6-2

複数 6-4

リポート後の設定の保存 6-12

トランスフォーム セット

説明 7-15

に

認証

注意事項 4-15

ファブリック セキュリティ 8-1

ユーザ ID 4-3

リモート 4-3, 4-15

ローカル 4-3

認証、許可、アカウントینگ。「AAA」を参照

ね

ネットワーク オペレータ

権限 4-4

ネットワーク管理者

権限 4-4

追加のロール 4-4

は

ハイ アベイラビリティ

DHCHAP との互換性 8-3

パスワード

DHCHAP 8-4, 8-5

強力な特性 3-6

ふ

ファイバチャネル インターフェイス

デフォルト設定 3-7, 4-16, 6-6, 7-22, 8-6, 9-10, 10-3

ファブリック セキュリティ

デフォルト設定 8-6

認証 8-1

ファブリック バインディング

DHCHAP との互換性 8-3

EFMD 10-1

Ex ポートの確認 10-2

実行 10-2

説明 ?? ~ 10-2

デフォルト設定 10-3

ポート セキュリティとの比較 10-1

ディセーブル化 9-14

データベースからのエントリの削除 (手順) 9-19

データベースのコピー 9-21

データベースの削除 9-22

データベースのシナリオ 9-8

データベースの消去 9-22

データベースの相互作用 9-8

データベース マージの注意事項 9-9

デフォルト設定 9-10

統計情報の表示 (手順) 9-24

非アクティブ化 9-15

ファブリック バインディングとの比較 10-1

ポート セキュリティ 自動学習

CFS 使用時の設定の注意事項 9-11

CFS を使用しない設定の注意事項 9-11

イネーブル化 9-4

設定の配信 9-6

説明 9-2

ディセーブル化 9-18

デバイスの許可 9-4

ポート セキュリティ データベース

コピー 9-21

コンフィギュレーション データベースへのアクティブ データベースのコピー (手順) 9-17

再アクティブ化 9-16

削除 9-22

シナリオ 9-8

手動設定時の注意事項 9-12

消去 9-22

相互作用 9-8

マージに関する注意事項 9-9

ポートチャネル

DHCHAP との互換性 8-3

ホスト名

デジタル証明書の設定 6-7

へ

ベンダー固有属性。「VSA」を参照

ほ

ポート セキュリティ

CFS 配信の設定 ?? ~ 9-7

DHCHAP との互換性 8-3

WWN の識別 9-5

アクティブ化 9-3, 9-15

アクティブ化の拒否 9-3

イネーブル化 9-14

強制的なアクティブ化 9-15

実行メカニズム 9-2

自動学習 9-2

手動設定時の注意事項 9-12

設定の表示 (手順) 9-23

ゆ

ユーザ

アカウント情報の表示 **3-18**

削除（手順） **3-13**

設定 **3-12**

説明 **3-5**

ユーザ ID

認証 **4-3**

ユーザ アカウント

情報の表示 **3-18**

設定 **3-18**

パスワードの特性 **3-6**

ユーザ プロファイル

ロール情報 **4-4**

れ

連邦情報処理標準規格。「FIPS」を参照

ろ

ロール

削除（手順） **3-9**

設定 **3-2**

設定の配信 **3-18**

デフォルト権限 **4-4**

デフォルト設定 **3-8**

ユーザ プロファイル **4-4**

ロールの設定 **3-2**

「共通ロール」も参照

ロール データベース

Fabric Manager での表示 **3-17**

配信のイネーブル化 **3-11**

配信のディセーブル化 **3-11**

ログイン

SSH **4-5**

Telnet **4-5**