



## Symbols

- # (ナンバー記号) 11-6
- \* (ワイルドカード) 3-10, 5-8, 11-6

## A

### AAA

- アカウントティング 4-19
  - 設定 4-5
  - 認可 4-15
  - 認証 4-7
- aaa accounting コマンド 4-19
- aaa authentication コマンド 4-7
- aaa authorization コマンド 4-15
- action コマンド 7-31
- add-service コマンド 7-16
- admin 特権レベル 3-2
- always-accept 7-32
- always-ignore 7-32
- AP
  - アップグレード 13-17
  - アップグレード、インライン 13-23
  - ~からのブート 2-15
  - 設定の消去 13-29
  - パスワードの消去 13-29, 13-31
- arp コマンド 12-44

- auth パケットタイプ 7-18

## B

- boot コマンド 2-15

## C

- CFE 13-19, 13-25, 13-27
- clear ap config コマンド 13-29
- clear ap password コマンド 13-29, 13-31
- clear counters コマンド 3-14, 12-6
- clear log コマンド 12-14
- CLI
  - エラーメッセージ 3-7
  - コマンドのショートカット 3-9
  - コマンドの発行 3-5
  - 使用 3-2
  - タブ補完 3-8
  - プロンプトの変更 4-41
  - ヘルプの取得 3-8
- config 特権レベル 3-2
- copy guard-running-config コマンド 5-24, 5-27
- copy login-banner コマンド 4-51
- copy コマンド
  - ftp running-config 13-7

packet-dump 12-24  
 running-config 5-25, 13-4  
 ゾーンのログ 12-13  
 レポート 11-12  
 ログ 12-10, 12-13  
 copy-from-this 5-8  
 copy-policies コマンド 8-29  
 copy wbm-logo コマンド 4-53  
 cpu 使用率 12-40

## D

date コマンド 4-36  
 DDoS  
   概要 1-3  
 deactivate コマンド 8-11, 9-6  
 default-gateway コマンド 3-15  
 description コマンド 5-10  
 detect learning コマンド 8-10  
 detect コマンド 9-6  
 diff コマンド 8-25, 8-26  
 disable コマンド 7-12  
 Distributed Denial of Service  
   「DDoS」を参照  
 DNS  
   TCP プロトコルフロー 11-8  
   TCP ポリシー テンプレート 7-5  
   検出された異常 11-3  
 dst トラフィック特性 7-19  
 dst-ip-by-ip アクティベーション形態 9-4, 9-10  
 dst-ip-by-name アクティベーション形態 9-4  
 dynamic 特権レベル 3-2

## E

enable  
   password コマンド 4-14  
   コマンド 4-15, 7-12  
 entire-zone アクティベーション形態 9-4  
 event monitor コマンド 12-9  
 export sync-config コマンド 5-26  
 export コマンド 13-11  
   packet-dump 12-23, 12-24  
   レポート 11-11

## F

file-server  
   sync-config の表示 5-27, 13-12  
   コマンド 5-26, 13-2  
   削除 13-3  
   設定 13-2  
   表示 13-3, 13-13  
 first-hit 4-23  
 fixed-threshold 7-25  
 flash-burn コマンド 13-27  
 fragments 11-8  
   検出された異常 11-3  
   ポリシー テンプレート 7-5

## G

global トラフィック特性 7-20  
 Guard  
   設定のエクスポート 13-11  
   設定モード 3-4

- GUARD 設定、インポート 5-25
- GUARD 設定、エクスポート 5-24, 5-27
- GUARD 設定のインポート 5-25
- GUARD\_ゾーンテンプレート
  - ゾーンテンプレートに含まれるポリシーテンプレート 7-8
- Guard 保護のアクティベーション方式 9-4
- guard-conf コマンド 5-16
- GUARD\_DEFAULT 5-4
- GUARD\_LINK 5-4, 5-5
- GUARD\_TCP\_NO\_PROXY 5-5
- GUARD\_VOIP 5-5
  
- H
  
- histogram コマンド 7-35
- hostname
  - コマンド 4-41
  - 変更 4-41
- HTTP
  - 検出された異常 11-3
  - ポリシーテンプレート 7-5
- hw-module コマンド 2-14, 13-17, 13-18, 13-20, 13-24, 13-31
  
- I
  
- in パケットタイプ 7-18
- Interactive
  - 動作モード 10-7
  - ポリシーのステータス 7-33
- interactive-status コマンド 7-32
  
- IP address コマンド
  - 除外 5-12
- ip address コマンド
  - インターフェイス 3-12
  - 削除 5-13
  - ゾーン 5-12
- ip route コマンド 3-16
- IP アドレス
  - 変更、ゾーン 5-13
- IP しきい値設定 7-28
- IP スキャン 11-8
  - 検出された異常 11-3
  - ポリシーテンプレート 7-6
  
- K
  
- key publish コマンド 4-33, 4-34
- key コマンド
  - add 4-32, 4-37
  - generate 4-33, 4-40
  - remove 4-38
  
- L
  
- learning
  - policy-construction コマンド 8-7
  - threshold-tuning コマンド 8-10, 8-11
  - 結果の同期 8-5
  - コマンド 8-8, 8-13
  - しきい値の調整 8-10
  - プロセスの終了 8-8, 8-13
  - ポリシーの構築 8-6

- learning accept コマンド 8-8, 8-12
- learning-params
  - periodic-action コマンド 5-19, 8-8, 8-12, 8-16
  - periodic-action コマンドの無効化 8-8
  - threshold-multiplier コマンド 7-26
  - threshold-selection コマンド 8-12, 8-17
  - threshold-tuned コマンド 5-13, 8-19
  - 定期的なアクションの非アクティブ化 8-12
- learning-params fixed-threshold コマンド 7-25
- learning-params コマンド 5-18, 5-27
- LINK テンプレート 8-6
- logging コマンド 12-10
- login-banner コマンド 4-50
  
- M**
- max-services コマンド 7-11
- MIB、サポートされている 4-2
- min-threshold コマンド 7-11
- MP
  - アップグレード 13-20
  - アップグレード、インライン 13-23
  - ～からのブート 2-15
- mtu コマンド 3-12
  
- N**
- netstat コマンド 12-47
- no learning コマンド 8-8, 8-13
- non\_estb\_conns パケット タイプ 7-19
- notify 11-6
- notify ポリシー アクション 7-31
  
- ns ポリシー テンプレート 7-8
  
- O**
- other\_protocols
  - 検出された異常 11-3
- out\_pkts パケット タイプ 7-19
  
- P**
- packet-dump
  - auto-capture コマンド 12-17
  - エクスポート 12-23, 12-24, 13-11
  - シグニチャ 12-32
  - 自動
    - アクティブ化 12-17
    - 非アクティブ化 12-20
    - 設定の表示 12-20
- packet-dump コマンド 12-20
- permit
  - コマンド 3-18, 3-20, 4-3
- permit ssh コマンド 4-31
- ping コマンド 12-53
- pkts パケット タイプ 7-19
- policy set-timeout コマンド 7-30
- policy-template add-service コマンド 7-16
- policy-template remove service コマンド 7-17
- policy-type アクティベーション形態 9-5
- power enable コマンド 2-15
- protect コマンド 9-6
- protection-end-timer 9-10, 9-13
- protect-ip-state コマンド 9-5

protocol トラフィック特性 7-20

## R

reactivate-zones 13-13

reload コマンド 13-13

remote-activate ポリシー アクション 7-31

remote-guard コマンド 9-11, 9-12

remove service コマンド 7-16

reqs パケット タイプ 7-19

reset コマンド 2-14

RTP/RTCP 5-5

running-config

copy 5-25, 13-4, 13-7

show 12-2

## S

scanners トラフィック特性 7-20

service

copy 8-29

wbm 3-18

コマンド 3-18

session-timeout コマンド 4-55

set-action 7-31

show public-key コマンド 4-40

show コマンド

cpu 12-40

diagnostic-info 12-37

dynamic-filters 6-22

file-server 13-3, 13-13

host-keys 4-32, 4-36

learning-params 7-26

log export-ip 12-12

login-banner 4-50

memory 12-39

packet-dump 12-20

packet-dump signatures 12-32

policies statistics 8-14

recommendations pending-filters 10-5, 10-10

remote-guards 9-11, 9-12

running-config 12-2

show 12-3

sync-config file-servers 5-27, 13-12, 13-13

sync-config 5-27

カウンタ 12-4

公開鍵 4-36, 4-40

推奨事項 10-8, 10-9

ゾーンのポリシー 7-39

テンプレート 5-8

動的フィルタのソート 6-22

フレックスコンテンツ フィルタ 6-15

ポリシー 7-39

ポリシーの統計情報 7-41

モジュール 2-2, 13-17, 13-20, 13-21

ラーニング 8-15

レート 12-4

レポートの詳細 11-7

ロギング 12-12

ログ 12-12

show 特権レベル 3-2

shutdown コマンド 3-13

SIP

ゾーン テンプレート 5-5

- ポリシー テンプレート 7-7
- snapshot
  - コマンド 8-24
  - 削除 8-28
  - 比較 8-25
  - 表示 8-27
  - 保存する 8-24, 8-25
  - ポリシーのバックアップ 7-44, 8-25, 8-30
- snapshot コマンド 8-23
- SNMP
  - アクセス 4-2
  - トラップ ジェネレータの設定 4-42
  - トラップの説明 4-44
- snmp コマンド
  - community 4-49
  - trap-dest 4-42
- SPAN、設定 2-9
- speed コマンド 3-13
- src トラフィック特性 7-20
- SSH
  - 鍵の削除 4-38
  - 鍵の生成 4-33, 4-40
  - 公開鍵の表示 4-36
  - サービス 3-20
  - 設定 3-20
  - ホスト鍵 4-35
- ssh キー、パブリッシュ 4-34
- state コマンド 7-23
- syn\_by\_fin パケット タイプ 7-19
- sync コマンド 5-20, 5-22
- syms パケット タイプ 7-19
- syslog
  - エクスポート パラメータの設定 12-10
  - サーバの設定 12-11
  - メッセージの形式 12-10
- T
- TACACS+
  - 検索の設定 4-23
  - サーバの IP アドレス 4-21
  - サーバの暗号鍵 4-22
  - サーバの接続タイムアウト 4-24
  - サーバの設定 4-20
  - 統計情報のクリア 4-25
  - 統計情報の表示 4-25
  - 認証
    - key generate コマンド 4-28
    - key publish コマンド 4-33
- tacacs-server コマンド
  - clear statistics 4-25
  - first-hit 4-20, 4-23
  - 鍵 4-20, 4-22
  - タイムアウト 4-20, 4-24
  - 統計情報の表示 4-25
  - ホスト 4-20, 4-21
- TCP
  - 検出された異常 11-3, 11-8
  - プロキシが使用されない場合のポリシー テンプレート 7-8
  - ポリシー テンプレート 7-6
  - thresh-mult 7-27
  - threshold
    - IP しきい値の設定 7-28

- 受け入れ前の乗算 7-26
  - 固定値として設定 7-25
  - コマンド 7-24
  - 選択 8-24
  - 調整 1-6, 8-3
  - 調整済みのマーク付け 5-13, 8-19
  - 特定の IP の設定 7-28
  - リストの設定 7-29
  - ワーム 7-34
  - threshold-list コマンド 7-29
  - threshold-selection 8-12
  - timeout コマンド 7-30
  - traceroute コマンド 12-51
  - trap-dest 4-42
- U**
- UDP
    - 検出された異常 11-4
    - ポリシー テンプレート 7-7
  - unauth\_pkts パケット タイプ 7-19
  - upgrade コマンド 13-30
  - username
    - 暗号化されたパスワード 4-9
  - username コマンド 4-9
- V**
- VACL、設定 2-6
  - Voice over IP
    - VoIP を参照
- VoIP**
- ゾーン テンプレート 5-5
  - ポリシー テンプレート 7-7
- W**
- WBM
    - アクティブ化 3-18
  - WBM ログ
    - 削除 4-54
    - 追加 4-53
  - worm\_tcp ポリシー テンプレート 7-9
- X**
- XML スキーマ 11-11?11-14, 12-24, 13-11
- Z**
- zone
    - コマンド 10-7
- あ**
- アイドルセッション、タイムアウトの設定 4-55
  - アイドルセッション、タイムアウトの表示 4-55
  - アカウントティング、設定 4-18
  - アクションフロー 11-10
  - アップグレード
    - AP 13-17
    - MP 13-20
    - インライン 13-23

アプリケーションパーティション  
「AP」を参照

## い

### 異常

検出された 11-3

フロー 11-6

異常検出エンジンのメモリ使用率 12-39, 12-42

### イベントログ

アクティブ化 12-9

非アクティブ化 12-9

### インターフェイス

IP アドレスの設定 3-12

アクティブ化 3-11, 3-13

カウンタのクリア 3-14

コマンド 3-12

設定モード 3-3

インタラクティブ検出モード 1-7, 9-3

インタラクティブ保護モード 9-3

### インポート

設定 13-7

インラインアップグレード 13-23

## え

### エクスポート

自動でのディセーブル化 13-12

設定ファイル 13-4

レポートを自動的に 11-11

ログファイル 12-13

エクスポート、GUARD 設定の 5-24, 5-27

## か

### カウンタ

クリア 3-14, 12-6

履歴 12-4

カウンタ、表示 12-4

### 監視

ネットワークトラフィック 12-23, 12-24

### 管理

SSH 3-20

VLAN 2-4

WBM 3-18

概要 3-18

ポート 2-4, 3-11, 3-12

## き

キャプチャ、パケット 12-20

## く

グローバルモード 3-3

## け

### 検出

インタラクティブモード 1-7, 9-3

自動モード 1-7, 9-3

### 検出された

異常 11-3

フロー 11-10

検出された攻撃 11-8



- 検出レベル
  - 分析 7-18
  
- こ
  
- 公開鍵
  - 表示 4-40
- 攻撃のタイプ
  - 検出された攻撃 11-8
- 攻撃レポート
  - notify 11-6
  - エクスポート 11-11, 13-11
  - エクスポート、自動的に 11-11
  - 検出された異常 11-3
  - コピー 11-12
  - タイミング 11-2
  - 統計情報 11-3
  - 表示 11-7
  - レイアウト 11-2
- コマンドのショートカット 3-9
- コマンドの無効化
  - コマンド、無効化 3-7
- コマンド補完 4-18
- コマンドライン インターフェイス
  - 「CLI」を参照 3-2
  
- さ
  
- サービス
  - snmp-trap 4-42
  - アクセス権 4-3
  - イネーブル化 4-3
  
- コマンド 4-3
- 削除 7-16
- 追加 7-15
- サービスのイネーブル化 4-3
  
- し
  
- しきい値の調整
  - 結果を定期的に保存 8-16
- シグニチャ
  - 生成 12-31
  - シグニチャの生成 12-31
  - シグニチャの抽出 12-31
- 時刻、設定 4-36
- システム ログ
  - メッセージの形式 12-10
- 自動検出モード 1-7, 9-3
- 自動保護モード 9-3
  
- す
  
- 推奨事項
  - アクティブ化 10-7, 10-11
  - 受け入れ 10-12
  - 概要 10-2
  - 決定の変更 7-32
  - コマンド 10-11
  - 通知の受信 10-2
  - 非アクティブ化 10-6, 10-14
  - 表示 10-2, 10-8
  - 保留フィルタの表示 10-5, 10-10
  - 無視 10-12

スーパーバイザ エンジン

シャットダウン 2-14

設定 2-1

設定の確認 2-16

設定の保存 2-1

電源の切断 2-15

ブート 2-15

リセット 2-14

スーパーバイザ モジュール

サポートされているバージョン 13-14

スタティック ルート

追加 3-16

スナップショット

定期的に保存 8-16

せ

セッション、アイドル タイムアウトの表示 4-55

セッション タイムアウト、ディセーブル化 4-55

セッション、タイムアウトの設定 4-55

設置

確認 2-2

設定

インポート 13-7

スーパーバイザ エンジンの保存 2-1

ファイル

インポート 13-7

エクスポート 13-4

コピー 13-4

表示 12-2

設定、コマンド モードへのアクセス 4-17

設定コマンド 3-11

設定モード 3-3

そ

ゾーン

IP アドレス 5-12

IP アドレスの削除 5-13

IP アドレスの除外 5-12

IP アドレスの定義 5-12

IP アドレスの変更 5-13

LINK テンプレート 8-6

オフラインでの同期 5-23

カウンタのクリア 12-6

検出 9-2

コピー 5-8

コマンド 5-6, 5-8

コマンド補完 4-18, 5-10

再設定 5-10

削除 5-8

作成 5-6

自動的な同期 5-18

ステータスの表示 12-3

設定のエクスポート 5-26

設定の同期 5-14

設定の表示 5-11

設定モード 3-4, 5-10

定義 1-4

テンプレート 5-3

動作モード 5-8

比較 8-26

複製 5-8

ポリシーの表示 7-39

- ラーニング 8-2
- ゾーンのポリシー
  - 調整済みのマーク付け 5-13, 8-19
- た
- タイムアウトセッション、設定 4-55
- タイムアウトセッション、ディセーブル化 4-55
- ち
- 注意
  - 記号の概要 xix
- 注釈
  - 記号の概要 xx
- て
- 定期的なアクション
  - 非アクティブ化 8-8, 8-12
  - ポリシーの自動受け入れ 8-8, 8-12
- ディセーブル化
  - 自動エクスポート 13-12
- デフォルト設定、～に戻す 13-29
- テンプレート
  - LINK 8-6
  - ゾーン 5-3
  - ポリシーの表示 5-8
- と
- 同期
  - 設定のエクスポート 13-11
- 動的フィルタ
  - 1000 以上 6-23
  - イベントの表示 12-11
  - 概要 6-2, 6-22
  - コマンド 6-26, 6-27, 9-13
  - 削除 6-27
  - ソート 6-22
  - 定義 1-8
  - ～の作成の防止 6-28
  - 表示 6-22
  - ワーム 7-37
- 特定の IP しきい値 7-28
- 特権レベル 3-2
  - ～の間の移動 4-14
  - パスワードの割り当て 4-14
- トラップ 12-10
- トラフィック
  - 監視 12-23, 12-24
- トラフィックの送信元
  - SPAN 2-5
  - VACL 2-5
  - キャプチャ 2-5
  - 設定 2-5
- に
- 認可
  - ゾーン コマンド補完のディセーブル化 4-18, 5-10
- 認可、設定 4-12, 4-13
- 認証、設定 4-7
- 認証されていない TCP の検出された異常 11-4

- ね
- ネットワーク サーバ
    - sync-config の表示 5-27, 13-12
    - 削除 13-3
    - 設定 13-2
    - 表示 13-3, 13-13
  - ネットワーク サーバ、sync-config の表示 13-13
- は
- バークリー パケット フィルタ 6-12
  - バージョン、アップグレード 13-30
  - バイパス フィルタ
    - コマンド 6-18
    - 削除 6-21
    - 設定 6-18
    - 定義 1-8, 6-2
    - 表示 6-20
  - ハイブリッド 11-8
  - パケット、キャプチャ 12-20
  - パスワード
    - 暗号化された 4-9
    - イネーブル化 4-14
    - 復旧 13-29, 13-31
    - 変更 4-10
  - パスワード、復旧 13-31
  - バナー
    - ログインの設定 4-50
- ひ
- ヒント
    - 記号の概要 xx
- ふ
- ファイル サーバ
    - 設定 13-2
  - ファイル サーバ、sync-config の表示 13-13
  - ファシリティ 12-10
  - フィルタ
    - 概要 6-2
    - 動的 1-8, 6-2, 6-22
    - バイパス 1-8, 6-18
    - フレックスコンテンツ 1-8, 6-4
  - フラッシュの焼き付け 13-27
  - フレックスコンテンツ フィルタ
    - 設定 6-5
    - 定義 1-8, 6-2
    - 番号変更 6-5
    - 表示 6-15
    - フィルタリング基準 6-4
  - フレックスコンテンツ フィルタの番号変更 6-5
  - プロキシ
    - プロキシが使用されない場合のポリシー テンプレート 7-8
    - プロキシが使用されない場合のポリシー テンプレート 7-8
    - 分析検出レベル 7-18

- ほ
- ポート
    - 管理 3-11, 3-12
    - データ 3-11, 3-12
  - ポート スキャン 11-8
    - 検出された異常 11-3
    - ポリシー テンプレート 7-6
  - 他のプロトコル
    - ポリシー テンプレート 7-6
  - 保護
    - アクティベーション方式 9-4
    - 非アクティブ化 9-6
  - ホスト、ロギング 12-11
  - ホスト鍵
    - 削除 4-30, 4-32
  - ポリシー
    - copy-policies 8-29
    - learning-params fixed-threshold コマンド 7-25
    - threshold 7-4, 7-22, 7-24
    - threshold-list コマンド 7-29
    - アクション 7-22, 7-31
    - アクティブ化 7-22
    - 現在の～のバックアップ 7-44, 8-25, 8-30
    - 構造 7-2
    - 構築 1-6, 7-4, 8-3, 8-6
    - コマンド 7-21
    - サービスの削除 7-16
    - サービスの追加 7-15
    - しきい値の乗算 7-27
    - しきい値の調整 1-6, 7-4, 8-3, 8-10
    - しきい値を固定 7-25
    - 状態 7-22
    - 設定モード 3-4
    - タイムアウト 7-22, 7-30
    - 調整済みのマーク付け 5-13, 8-19
    - ディセーブル化 7-22
    - 統計情報の表示 7-41, 8-14
    - トラフィック特性 7-19
    - ナビゲーションパス 7-21
    - パケットタイプ 7-18
    - パラメータのコピー 8-29
    - 非アクティブ化 7-22
    - ワイルドカードの使用 7-22, 7-39, 7-42
  - ポリシー テンプレート
    - max-services 7-11
    - min-threshold 7-11
    - worm\_tcp 7-9
  - 概要 7-5, 7-14
  - コマンド 7-8, 7-9, 7-12
  - 状態 7-12
  - 設定コマンド レベル 7-9
  - 設定モード 3-4
  - 同期化のための Guard ポリシー テンプレート 7-8
  - パラメータ 7-9
  - リストの表示 7-8
  - ポリシーの構築 8-6
  - ポリシーのしきい値の調整 8-10
  - 保留動的フィルタ
    - 表示 10-5, 10-10
- め
- メモリ消費量 12-39
  - メモリ使用率、異常検出エンジン 12-39, 12-42

メンテナンス パーティション  
「MP」を参照

## ゆ

ユーザ

username コマンド 4-9

新しい~の追加 4-9

検出された異常 11-4

削除 4-11

システム ユーザ

Admin 2-13

riverhead 2-13

追加 4-9

特権レベル 3-2, 4-13

特権レベルの割り当て 4-8

ユーザ フィルタ

コマンド 6-5

## ら

ラーニング

概要 8-2

ラーニング パラメータ、表示する 8-15

## り

リポート

パラメータ 13-13

リモート Guard

アクティブ化 6-25

リモート Guard リスト

表示 9-11, 9-12

リモートの Guard

アクティブ化 9-7

デフォルト リスト 9-11

保護の終了 9-10, 9-13

リスト 9-12

リストのアクティベーション順序 9-12

## る

ルータ設定モード 3-4

ルーティング テーブル

操作 3-16

表示 3-17

## れ

レート

履歴 12-4

レート、表示 12-4

レポート

エクスポート 13-11

「攻撃レポート」を参照 11-2

詳細 11-7

## ろ

ロギング、設定の表示 12-12

ログ ファイル

エクスポート 12-10, 12-13

クリア 12-14

表示 12-12

ログイン バナー

インポート 4-51

- 削除 4-52
- 設定 4-50
- ロゴ、WBM の削除 4-54
- ロゴ、WBM の追加 4-53

## わ

### ワーム

- 概要 7-34
  - 攻撃の識別 7-37
  - しきい値 7-34, 7-35
  - 動的フィルタ 7-37
  - ポリシー 7-19, 7-20
  - ポリシー テンプレート 7-7, 7-35
- ワンポイントアドバイス
- 記号の概要 xx