



Symbols

- # (ナンバー記号) 11-6
- * (ワイルドカード) 3-9, 5-9, 11-6

Numerics

- 1 Gbps および 2 Gbps 帯域幅オプション
 - 2 Gbps へのアップグレード 13-30
 - 説明 1-9
 - ソフトウェア バージョンの表示 12-3
 - ソフトウェア ライセンス キーの表示 12-4
- 2 Gbps 動作のアップグレード
 - SSL 証明書の再生成 13-33
 - 追加データ ポートのアクティブ化 13-33

A

AAA

- アカウントिंग 4-20
 - 設定 4-5
 - 認可 4-16
 - 認証 4-7
- aaa accounting コマンド 4-20
- aaa authentication コマンド 4-7
- aaa authorization コマンド 4-16
- action コマンド 7-31

- add-service コマンド 7-16
- admin 特権レベル 3-2, 4-9
- always-accept 7-33
- always-ignore 7-33

AP

- アップグレード 13-17
- アップグレード、インライン 13-24
- 設定の消去 13-34
- パスワードの消去 13-34, 13-36
- ～へのブート 2-19
- auth パケット タイプ 7-18

B

- boot コマンド 2-19

C

- CFE 13-19, 13-26, 13-28
- clear ap config コマンド 13-34
- clear ap password コマンド 13-34, 13-36
- clear counters コマンド 3-13, 12-10
- clear log コマンド 12-18
- 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 4-42
 - ヘルプの取得 3-8
- config 特権レベル 3-2, 4-9
- copy guard-running-config コマンド 5-25, 5-28
- copy login-banner コマンド 4-52
- copy wbm-logo コマンド 4-54
- copy コマンド
 - ftp running-config 13-7
 - packet-dump 12-27
 - running-config 5-26, 13-4
 - ゾーンのログ 12-16
 - レポート 11-12
 - ログ 12-13, 12-16
- copy-from-this 5-9
- copy-policies コマンド 8-28
- CPU 使用率 12-42

- D
- DDoS
 - 概要 1-3
- deactivate コマンド 8-11, 9-7
- default-gateway コマンド 3-14
- description コマンド 5-11
- detect learning コマンド 8-10
- detect コマンド 9-7
- DETECTOR_DEFAULT 5-3
- DETECTOR_WORM 5-3
- 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 9-5, 9-11
- dst-ip-by-name アクティベーション形態 9-5
- dynamic 特権レベル 3-2, 4-9

- 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 9-5
- event monitor コマンド 12-13
- export sync-config コマンド 5-27
- export コマンド 13-10
 - packet-dump 12-26, 12-27
 - reports 11-11

- F
- file-server
 - コマンド 5-27, 13-2
 - 設定 13-2
 - sync-config の表示 5-28, 13-12
 - 削除 13-3
 - 表示 13-3, 13-13

- fixed-threshold 7-26
 - flash-burn コマンド 13-28
 - 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 13-10
 - 設定モード 3-4
 - GUARD 設定、インポート 5-26
 - GUARD 設定、エクスポート 5-25, 5-28
 - 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 7-7
 - Guard 保護のアクティベーション方式 9-5
 - guard-conf コマンド 5-17
 - GUARD_DEFAULT 5-4
 - GUARD_LINK 5-4, 5-5
 - GUARD_TCP_NO_PROXY 5-5
- ## H
- histogram コマンド 7-35
 - hostname
 - コマンド 4-42
 - 変更 4-42
 - 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 2-17, 13-18, 13-19, 13-21, 13-25, 13-36
- ## I
- in パケット タイプ 7-18
 - Interactive
 - 動作モード 10-6
 - ポリシーのステータス 7-33
 - interactive-status コマンド 7-33
 - ip address コマンド
 - インターフェイス 3-12
 - 削除 5-14
 - 除外 5-13
 - ゾーン 5-13
 - ip route コマンド 3-15
 - IP アドレス
 - 変更、ゾーン 5-14
 - IP しきい値設定 7-29
 - 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 4-34, 4-35
 - key コマンド
 - add 4-34, 4-38
 - generate 4-35, 4-40
 - remove 4-39

- L**
- learning
 - policy-construction コマンド 8-7
 - threshold-tuning コマンド 8-10, 8-11
 - コマンド 8-8, 8-13
 - learning accept コマンド 8-8, 8-12
 - learning-params
 - periodic-action コマンド 5-20, 8-8, 8-12, 8-16
 - periodic-action コマンドの無効化 8-8
 - threshold-multiplier コマンド 7-27
 - threshold-selection コマンド 8-12, 8-17
 - threshold-tuned コマンド 5-14, 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 7-26
 - learning-params コマンド 5-19, 5-28
 - LINK テンプレート 8-6
 - logging コマンド 12-14
 - login-banner コマンド 4-51
- M**
- max-services コマンド 7-11
 - MDM
 - アクティブ化 3-19
 - min-threshold コマンド 7-11
 - MP
 - アップグレード 13-21
 - アップグレード、インライン 13-24
 - ～へのブート 2-19
 - 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 7-32
 - ns ポリシー テンプレート 7-8
- O**
- out_pkts パケット タイプ 7-19
- P**
- packet-dump
 - auto-capture コマンド 12-22
 - エクスポート 12-26, 12-27, 13-10
 - シングニチャ 12-34
 - 自動
 - アクティブ化 12-20
 - 非アクティブ化 12-23
 - 設定の表示 12-23
 - packet-dump コマンド 12-23
 - permit
 - コマンド 3-17, 3-20, 4-3
 - permit ssh コマンド 4-33
 - ping コマンド 12-53
 - pkts パケット タイプ 7-19
 - policy set-timeout コマンド 7-31
 - policy-template add-service コマンド 7-16
 - policy-template remove service コマンド 7-17
 - policy-type アクティブーション形態 9-6

- power enable コマンド 2-18
 - protect コマンド 9-7
 - protection-end-timer 9-11, 9-14
 - protect-ip-state コマンド 9-6
 - 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 7-32
 - remote-guard コマンド 9-12, 9-13
 - remove service コマンド 7-16
 - reqs パケット タイプ 7-19
 - reset コマンド 2-18
 - running-config
 - copy 5-26, 13-4, 13-7
 - show 12-5
- ## S
- scanners トラフィック特性 7-20
 - service
 - MDM 3-19
 - snmp-trap 4-43
 - WBM 3-17
 - コマンド 3-17, 3-19, 4-3
 - session-timeout コマンド 4-56
 - set-action 7-32
 - show public-key コマンド 4-41
 - show コマンド
 - cpu 12-42
 - diagnostic-info 12-39
 - dynamic-filters 6-22
 - file-server 13-3, 13-13
 - host-keys 4-33, 4-37
 - learning-params 7-26
 - log export-ip 12-15
 - login-banner 4-51
 - memory 12-41
 - packet-dump 12-23
 - packet-dump signatures 12-34
 - public-key 4-37, 4-40
 - recommendations pending-filters 10-5, 10-9
 - remote-guards 9-12, 9-13
 - running-config 12-5
 - show 12-7
 - sync-config 5-28
 - sync-config file-servers 5-28, 13-12, 13-13
 - カウンタ 12-8
 - 推奨事項 10-7, 10-8
 - ゾーンのポリシー 7-39
 - テンプレート 5-9
 - 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 6-14
 - ポリシー 7-39
 - ポリシーの統計情報 7-41, 8-14
 - モジュール 2-3, 13-18, 13-21, 13-22
 - ラーニング パラメータ 8-15
 - レート 12-8
 - レポートの詳細 11-7
 - ロギング 12-15
 - ログ 12-16
 - show 特権レベル 3-2, 4-9

- shutdown コマンド 3-12
 - snapshot コマンド 8-22
 - SNMP
 - トラップ ジェネレータの設定 4-43
 - トラップの説明 4-45
 - snmp コマンド
 - community 4-50
 - trap-dest 4-43
 - SPAN、設定 2-12
 - src トラフィック特性 7-20
 - SSH
 - 鍵の削除 4-39
 - 鍵の生成 4-35, 4-40
 - 公開鍵の表示 4-37
 - サービス 3-20
 - 設定 3-20
 - ホスト鍵 4-36
 - ssh 鍵、パブリッシュ 4-35
 - state コマンド 7-23
 - syn_by_fin パケット タイプ 7-19
 - sync コマンド 5-22, 5-23
 - 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 12-14
 - サーバの設定 12-15
 - メッセージの形式 12-14
- T
- TACACS+
 - サーバの IP アドレス 4-24
 - サーバの暗号鍵 4-24
 - サーバの接続タイムアウト 4-26
 - サーバの設定 4-22
 - 統計情報のクリア 4-27
 - 統計情報の表示 4-27
 - 認証
 - key generate コマンド 4-29
 - key publish コマンド 4-34
 - tacacs-server コマンド
 - clear statistics 4-27
 - first-hit 4-22
 - host 4-22, 4-24
 - key 4-22, 4-24, 4-25
 - show statistics 4-27
 - timeout 4-22, 4-26
 - 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 7-28
 - threshold
 - コマンド 7-25
 - 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 4-43
- 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 13-35
 username コマンド 4-9

V

VACL、設定 2-7

W

WBM

アクティブ化 3-17

WBM ログ

削除 4-55

追加 4-54

worm_tcp ポリシー テンプレート 7-9

X

XG ソフトウェア イメージ、2 Gbps 動作
 ソフトウェア イメージの取得 13-31

XG ソフトウェア バージョン、2 Gbps 動作 13-30

XG ソフトウェア ライセンス キー 13-31

XML スキーマ 11-11?11-14, 12-26, 13-11

Z

zone

コマンド 5-7, 5-9

コマンド補完 4-19, 5-11

あ

アイドルセッション、タイムアウトの設定 4-56

アイドルセッション、タイムアウトの表示 4-56

アカウンティング、設定 4-20

アクションフロー 11-10

アップグレード

AP 13-17

MP 13-21

インライン 13-24

アップグレードライセンス 13-31

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 11-5

異常検出エンジンのメモリ使用率 12-41, 12-44

イネーブル化、サービスの 4-3

イベント ログ

アクティブ化 12-13

非アクティブ化 12-13

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, 3-12

カウンタのクリア 3-13

コマンド 3-11

設定モード 3-3

インタラクティブ検出モード 1-7, 9-4

インタラクティブ保護モード 9-4

インポート

設定 13-7

インポート、GUARD 設定の 5-26

インラインアップグレード 13-24

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 12-16

エクスポート、GUARD 設定の 5-25, 5-28

か

カウンタ

クリア 3-13, 12-10

履歴 12-8

カウンタ、表示 12-8

監視

ネットワーク トラフィック 12-26, 12-27

管理

MDM 3-19

SSH 3-20

VLAN 2-5

WBM 3-17

概要 3-17

ポート 2-5

き

キー

生成、ライセンス用 13-31

キャプチャ、パケット 12-23

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, 9-4

自動モード 1-7, 9-4

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

エクスポート 11-11, 13-10

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
- 通知 11-6
- 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 4-19
- 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

- アクセス権 4-3
- イネーブル化 4-3
- コピー 8-28
- 削除 7-16
- 追加 7-15

し

しきい値

- IP しきい値の設定 7-29
- 受け入れ前の乗算 7-27
- 固定値として設定 7-25
- 選択 8-23
- 調整 1-6, 8-3
- 調整済みのマーク付け 5-14, 8-19
- 特定の IP の設定 7-29
- リストの設定 7-29

- ワーム 7-34
- しきい値の調整
 - 結果を定期的に保存 8-15
- シングニチャ
 - 生成 12-33
- システム ログ
 - メッセージの形式 12-14
- 自動検出モード 1-7, 9-4
- 自動保護モード 9-4

す

推奨事項

- アクティブ化 10-6, 10-10
- 受け入れ 10-11
- 概要 10-2
- 決定の変更 7-33
- コマンド 10-10
- 通知の受信 10-2
- 非アクティブ化 10-6, 10-13
- 表示 10-2, 10-7
- 保留フィルタの表示 10-5, 10-9
- 無視 10-11

スーパーバイザ エンジン

- シャットダウン 2-17
- 設定 2-1
- 設定の確認 2-20
- 設定の保存 2-1
- 電源の切断 2-18
- ブート 2-19
- リセット 2-18

スタティック ルート

追加 3-15

スナップショット

コマンド 8-23

削除 8-28

定期的に保存 8-15

比較 8-25

表示 8-26

保存 8-23, 8-24

ポリシーのバックアップ 7-44, 8-24, 8-30

せ

生成、シグニチャの 12-33

セッション、アイドル タイムアウトの表示 4-56

セッション タイムアウト、ディセーブル化 4-56

セッション、タイムアウトの設定 4-56

設置

確認 2-3

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 12-5

設定、コマンド モードへのアクセス 4-18

設定コマンド 3-10

設定モード 3-3

そ

ゾーン

IP アドレス 5-13

IP アドレスの削除 5-14

IP アドレスの除外 5-13

IP アドレスの定義 5-13

IP アドレスの変更 5-14

LINK テンプレート 8-6

オフラインでの同期 5-24

カウンタのクリア 12-10

検出 9-2

コピー 5-9

コマンド 10-6

再設定 5-11

削除 5-9

作成 5-7

自動的な同期 5-19

ステータスの表示 12-7

設定のエクスポート 5-27

設定の同期 5-15

設定の表示 5-12

設定モード 3-4, 5-11

テンプレート 5-3

動作モード 5-8

比較 8-26

複製 5-9

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 5-14, 8-19

ソフトウェア バージョン番号、表示 12-3

ソフトウェア ライセンス キー

キー情報の表示 12-4

た

帯域幅オプション

2 Gbps へのアップグレード 13-30

説明 1-9

ソフトウェア バージョンの表示 12-3

ソフトウェア ライセンス キーの表示 12-4

タイムアウトセッション、設定 4-56

タイムアウトセッション、ディセーブル化 4-56

ち

注意

記号の概要 xxi

注釈

記号の概要 xxii

抽出、シグニチャの 12-33

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 13-34

テンプレート

LINK 8-6

ゾーン 5-3

ポリシーの表示 5-9

と

同期

設定のエクスポート 13-10

動的フィルタ

1000 以上 6-23

イベントの表示 12-15

概要 6-2, 6-22

コマンド 6-26, 6-27, 9-14

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 7-29

特権レベル 3-2

～の間の移動 4-15

パスワードの割り当て 4-14

トラップ 12-14

トラフィック

監視 12-26, 12-27

トラフィックの送信元

SPAN 2-6

VACL 2-6

キャプチャ 2-6

設定 2-6

に

認可

zone コマンド補完のディセーブル化 4-19,
5-11

認可、設定 4-12, 4-14
 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 5-28, 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 13-35
 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 12-23
 パスワード
 暗号化された 4-10
 イネーブル化 4-14
 復旧 13-34, 13-36
 変更 4-10
 パスワード、復旧 13-36

バナー
 ログインの設定 4-51
 番号の割り当て直し、フレックスコンテンツ フィルタの 6-5

ひ

ヒント
 記号の概要 xxii

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 12-14
 フィルタ
 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 13-28
 フレックスコンテンツ フィルタ
 設定 6-5
 定義 1-8, 6-2
 番号の割り当て直し 6-5
 表示 6-14
 フィルタリング基準 6-4
 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 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
 - 検出された異常 11-3
 - 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 9-5
 - 非アクティブ化 9-7
 - ホスト、ロギング 12-15
 - ホスト鍵
 - 削除 4-32, 4-33
 - ポリシー
 - copy-policies 8-28
 - learning-params fixed-threshold コマンド 7-26
 - threshold 7-25
 - threshold-list コマンド 7-29
 - アクション 7-21, 7-31, 7-32
 - アクティブ化 7-22
 - 現在の～のバックアップ 7-44, 8-24, 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 7-4, 7-21
 - しきい値の乗算 7-28
 - しきい値の調整 1-6, 7-4, 8-3, 8-10
 - しきい値を固定 7-26
 - 状態 7-22
 - 設定モード 3-4
 - タイムアウト 7-21, 7-30
 - 調整済みのマーク付け 5-14, 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 8-28
 - 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 7-7
 - 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 10-2
 - 表示 10-5, 10-9
- め
- メモリ消費量 12-41
 - メモリ使用率、異常検出エンジン 12-41, 12-44

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 4-12

システム ユーザ

Admin 2-16

riverhead 2-16

追加 4-9

特権レベル 3-2, 4-14

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

ユーザ名

暗号化されたパスワード 4-10

ら

ラーニング

概要 8-2

結果の同期 8-5

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

ラーニング パラメータ、表示 8-15

ライセンス

XG アップグレード ライセンスの注文
13-31

キーの生成 13-31

り

リブート

パラメータ 13-13

リモート Guard

アクティブ化 6-25, 9-8

デフォルト リスト 9-12

保護の終了 9-11, 9-14

リスト 9-13

リストのアクティベーション順序 9-13

リモート Guard リスト

表示 9-12, 9-13

る

ルータ設定モード 3-4

ルーティング テーブル

操作 3-15

表示 3-16

れ

レート

履歴 12-8

レート、表示 12-8

レポート

「攻撃レポート」を参照 11-2

エクスポート 13-10

詳細 11-7

ろ

- ロギング、設定の表示 12-15
- ログファイル
 - エクスポート 12-13, 12-16
 - クリア 12-18
 - 表示 12-16
- ログインバナー
 - インポート 4-52
 - 削除 4-53
 - 設定 4-51
- ロゴ、WBM の削除 4-55
- ロゴ、WBM の追加 4-54

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 xxii