



INDEX

Symbols

- # (ナンバー記号) 11-4
- * (ワイルドカード) 3-7, 5-6, 11-4

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 13-20
 - 説明 1-9
 - ソフトウェア バージョンの表示 12-2
 - ソフトウェア ライセンス キーの表示 12-2
- 2 Gbps 動作のアップグレード
 - SSL 証明書の再生成 13-22
 - 追加データ ポートのアクティブ化 13-22

A

AAA

- アカウントティング 4-14
 - 設定 4-4
 - 認可 4-11
 - 認証 4-5
- aaa accounting コマンド 4-14
- aaa authentication コマンド 4-5
- aaa authorization コマンド 4-11
- action コマンド 7-20
- add-service コマンド 7-11
- admin 特権レベル 3-2, 4-7
- always-accept 7-22
- always-ignore 7-22

AP

- アップグレード 13-12
- アップグレード、インライン 13-16
- 設定の消去 13-23
- パスワードの消去 13-23, 13-24
- ～へのブート 2-12
- auth パケット タイプ 7-12

B

- boot コマンド 2-12

C

- CFE 13-13, 13-17, 13-18
- clear ap config コマンド 13-23
- clear ap password コマンド 13-23, 13-24
- clear counters コマンド 3-10, 12-6
- clear log コマンド 12-13
- CLI
 - エラー メッセージ 3-5
 - コマンドのショートカット 3-6
 - コマンドの発行 3-4
 - 使用 3-2
 - タブ補完 3-6
 - プロンプトの変更 4-28
 - ヘルプの取得 3-6
- config 特権レベル 3-2, 4-7
- copy guard-running-config コマンド 5-17, 5-19
- copy login-banner コマンド 4-34
- copy コマンド
 - ftp running-config 13-5
 - packet-dump 12-18
 - reports 11-8
 - running-config 5-17, 13-3
 - ゾーンのログ 12-12
 - ログ 12-10, 12-12
- copy-from-this 5-6
- copy-policies コマンド 8-18
- copy wbm-logo コマンド 4-36
- cpu 使用率 12-28

D

DDoS

- 概要 1-4
- スプーフィング攻撃 1-4

ゾンビ 1-4
 非スプーフィング攻撃 1-4
 deactivate コマンド 9-5
 default-gateway コマンド 3-11
 description コマンド 5-8
 detect コマンド 9-5
 DETECTOR_DEFAULT 5-3
 DETECTOR_WORM 5-3
 diff コマンド 8-16, 8-17
 disable コマンド 7-7
 DNS
 TCP プロトコル フロー 11-6
 TCP ポリシー テンプレート 7-3
 検出された異常 11-3
 dst トラフィック特性 7-13
 dst-ip-by-ip アクティベーション形態 9-4, 9-8
 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, 4-7

E

enable
 password コマンド 4-10
 コマンド 4-11, 7-7
 entire-zone アクティベーション形態 9-4
 event monitor コマンド 12-10
 export sync-config コマンド 5-19
 export コマンド 13-7
 packet-dump 12-18
 reports 11-8

F

file-server
 sync-config の表示 5-19, 13-8
 コマンド 5-18, 13-2
 削除 13-3
 設定 13-2
 表示 13-3, 13-9
 fixed-threshold 7-17
 flash-burn コマンド 13-19
 fragments 11-6
 検出された異常 11-3
 ポリシー テンプレート 7-3

G

global トラフィック特性 7-13
 Guard
 設定のエクスポート 13-7
 設定モード 3-3
 GUARD 設定、インポート 5-17
 GUARD 設定、エクスポート 5-17, 5-19
 GUARD 設定のエクスポート 5-17, 5-19
 GUARD_ゾーン ポリシー テンプレート 7-4
 Guard 保護のアクティベーション方式 9-4
 guard-conf コマンド 5-12
 GUARD_DEFAULT 5-3
 GUARD_LINK 5-3, 5-4
 GUARD_TCP_NO_PROXY 5-4

H

histogram コマンド 7-24
 hostname
 コマンド 4-28
 変更 4-28
 HTTP
 検出された異常 11-3
 ポリシー テンプレート 7-3
 hw-module コマンド 2-11, 13-12, 13-13, 13-14, 13-16,
 13-24

I

in パケット タイプ 7-12
 interactive
 動作モード 10-4
 ポリシーのステータス 7-22
 interactive-status コマンド 7-22
 ip address コマンド
 インターフェイス 3-9
 削除 5-10
 除外 5-9
 ゾーン 5-9
 ip route コマンド 3-12
 IP アドレス
 変更、ゾーン 5-9
 IP サマライズ 12-15, 12-16
 IP しきい値設定 7-19
 IP スキャン 11-6

検出された異常 11-3
 ポリシー テンプレート 7-3

K

key publish コマンド 4-23
 key コマンド
 add 4-22, 4-25
 generate 4-23, 4-27
 remove 4-25

L

learning accept コマンド 8-6, 8-9
 learning-params
 periodic-action コマンド 5-14, 8-6, 8-9, 8-11
 periodic-action コマンドの無効化 8-6
 threshold-multiplier コマンド 7-18
 threshold-selection コマンド 8-9, 8-12
 threshold-tuned コマンド 5-10, 8-13
 定期的なアクションの非アクティブ化 8-9
 learning-params fixed-threshold コマンド 7-17
 learning-params コマンド 5-14, 5-19
 LINK テンプレート 8-5
 logging コマンド 12-11
 login-banner コマンド 4-34

M

max-services コマンド 7-6
 MDM、アクティブ化 3-14
 min-threshold コマンド 7-7
 MP
 アップグレード 13-14
 アップグレード、インライン 13-16
 ～へのブート 2-12
 mtu コマンド 3-9

N

netstat コマンド 12-32
 no learning コマンド 8-6, 8-9
 non_estb_conns パケット タイプ 7-12
 notify 11-4
 notify ポリシー アクション 7-21

ns ポリシー テンプレート 7-5

O

other_protocols
 検出された異常 11-3
 ポリシー テンプレート 7-3
 out_pkts パケット タイプ 7-12

P

packet-dump
 auto-capture コマンド 12-16
 エクスポート 12-18, 13-7
 シングニチャ 12-23
 自動
 アクティブ化 12-15
 非アクティブ化 12-16
 設定の表示 12-16
 packet-dump コマンド 12-16
 permit
 コマンド 3-13, 3-15, 4-3
 permit ssh コマンド 4-22
 ping コマンド 12-36
 pkts パケット タイプ 7-13
 policy set-timeout コマンド 7-20
 policy-template add-service コマンド 7-11
 policy-template remove service コマンド 7-11
 policy-type アクティブ化形態 9-4
 power enable コマンド 2-11
 protect learning コマンド 8-8
 protect コマンド 9-5
 protection-end-timer 9-8, 9-9
 protect-ip-state コマンド 9-4
 protocol トラフィック 特性 7-13

R

reactivate-zones 13-9
 reload コマンド 13-9
 remote-activate ポリシー アクション 7-21
 remote-guard コマンド 9-8, 9-9
 remove service コマンド 7-11
 reports
 エクスポート 13-7

- 詳細 11-5
- reqs パケットタイプ 7-12
- reset コマンド 2-11
- running-config
 - copy 5-17, 13-3
 - show 12-3

- S**

- scanners トラフィック特性 7-13
- service
 - snmp-trap 4-29
- session-timeout コマンド 4-37
- set-action 7-21
- show public-key コマンド 4-27
- show コマンド
 - cpu 12-28
 - diagnostic-info 12-26
 - dynamic-filters 6-15
 - file-server 13-3, 13-9
 - host-keys 4-22, 4-24
 - learning-params 7-17
 - log export-ip 12-11
 - login-banner 4-34
 - memory 12-28
 - packet-dump 12-16
 - packet-dump signatures 12-23
 - public-key 4-24
 - recommendations pending-filters 10-3, 10-6
 - remote-guards 9-8, 9-9
 - running-config 12-3
 - show 12-4
 - sync-config file-servers 5-19, 13-8, 13-9
 - sync-config 5-19
 - カウンタ 12-5
 - 公開鍵 4-27
 - 推奨事項 10-5
 - ゾーンのポリシー 7-26
 - テンプレート 5-6
 - 動的フィルタのソート 6-15
 - フレックスコンテンツ フィルタ 6-9
 - ポリシー 7-26
 - ポリシーの統計情報 7-27, 8-10
 - モジュール 2-2, 13-12, 13-14
 - ラーニング パラメータ 8-11
 - レート 12-5
 - レポートの詳細 11-5
 - ロギング 12-11
 - ログ 12-11
 - show 特権レベル 3-2, 4-7
 - shutdown コマンド 3-9
 - snapshot
 - 概要 8-15
 - コマンド 8-15
 - 削除 8-18
 - 定期的に保存 8-11
 - 比較 8-16
 - 表示 8-17
 - 保存 8-15, 8-16
 - ポリシーのバックアップ 7-30, 8-20
- SNMP
 - トラップ ジェネレータの設定 4-29
 - トラップの説明 4-30
- snmp コマンド
 - community 4-33
 - trap-dest 4-29
- SPAN、設定 2-7
- src トラフィック特性 7-13
- SSH
 - 鍵の削除 4-25
 - 鍵の生成 4-23, 4-27
 - 公開鍵の表示 4-24
 - サービス 3-15
 - 設定 3-15
 - ホスト鍵 4-24
- ssh 鍵、パブリッシュ 4-23
- state コマンド 7-15
- syn_by_fin パケットタイプ 7-13
- sync コマンド 5-15, 5-16
- syms パケットタイプ 7-13
- syslog
 - エクスポート パラメータの設定 12-11
 - サーバの設定 12-11
 - メッセージの形式 12-10

- T**

- TACACS+
 - サーバの IP アドレス 4-15
 - サーバの暗号鍵 4-16
 - サーバの接続タイムアウト 4-17
 - サーバの設定 4-14

- 統計情報のクリア 4-17
 - 統計情報の表示 4-17
 - 認証
 - key generate コマンド 4-19
 - key publish コマンド 4-23
 - tacacs-server コマンド
 - clear statistics 4-17
 - first-hit 4-15
 - key 4-16
 - show statistics 4-17
 - timeout 4-15, 4-17
 - 鍵 4-15
 - ホスト 4-14, 4-15
 - TCP
 - 検出された異常 11-3, 11-6
 - プロキシが使用されない場合のポリシー テンプレート 7-5
 - ポリシー テンプレート 7-4
 - thresh-mult 7-18
 - threshold-list コマンド 7-19
 - threshold-selection 8-9
 - timeout コマンド 7-20
 - traceroute コマンド 12-35
 - trap-dest 4-29
- U**
- UDP
 - 検出された異常 11-3
 - ポリシー テンプレート 7-4
 - unauth_pkts パケット タイプ 7-13
 - upgrade コマンド 13-23
 - username
 - 暗号化されたパスワード 4-7
 - username コマンド 4-6
- V**
- VACL、設定 2-4
- W**
- WBM
 - アクティブ化 3-13
 - WBM ログ
 - 削除 4-37
 - 追加 4-36
 - worm_tcp ポリシー テンプレート 7-5
- X**
- XG ソフトウェア イメージ
 - ソフトウェア イメージの取得 13-20
 - ライセンス キー 13-20
 - XG ソフトウェア バージョン、2 Gbps 動作 13-20
 - XML スキーマ 11-8?11-10, 12-18, 13-7
- あ**
- アイドルセッション、タイムアウトの設定 4-37
 - アイドルセッション、タイムアウトの表示 4-37
 - アカウントिंग、設定 4-13
 - アクション フロー 11-7
 - アップグレード
 - AP 13-12
 - MP 13-14
 - インライン 13-15
 - アップグレード ライセンス 13-20
 - 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 11-2
 - フロー 11-4
 - 異常検出エンジンのメモリ使用率 12-28, 12-30
 - イベント ログ
 - アクティブ化 12-10
 - 非アクティブ化 12-10
 - インターフェイス
 - IP アドレスの設定 3-9
 - アクティブ化 3-8, 3-9
 - カウンタのクリア 3-10
 - コマンド 3-9
 - 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 10-1
 - インポート、GUARD 設定の 5-17
 - インライン アップグレード 13-15

え

エクスポート

設定ファイル 13-3

レポートを自動的に 11-8

ログファイル 12-12

エクスポート、自動でのディセーブル化 13-8

か

カウンタ

クリア 3-10, 12-6

履歴 12-5

カウンタ、表示 12-5

監視、ネットワークトラフィック 12-18

管理

MDM 3-14

SSH 3-15

VLAN 2-3

WBM 3-13

概要 3-13

ポート 2-3

き

キー、ライセンス用の生成 13-20

キャプチャ、パケット 12-16

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

検出された

異常 11-2

フロー 11-7

検出された攻撃 11-6

こ

公開鍵、表示 4-27

攻撃タイプ 11-6

攻撃レポート

notify 11-4

エクスポート 11-8, 13-7

エクスポート、自動的に 11-8

検出された異常 11-2

コピー 11-8

タイミング 11-2

統計情報 11-2

表示 11-5

レイアウト 11-2

コマンド、無効化 3-5

コマンドのショートカット 3-6

コマンドの無効化 3-5

コマンド補完 4-13

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

MDM 3-15

WBM 3-13

アクセス権 4-3

コピー 8-18

コマンド 3-13, 3-15, 4-2

削除 7-11

追加 7-10

サービス、イネーブル化 4-2

サービスのイネーブル化 4-2

し

しきい値

IP しきい値の設定 7-19

受け入れ前の乗算 7-18

固定値として設定 7-17

コマンド 7-17

選択 8-15

調整 1-6, 8-2

調整済みのマーク付け 5-10, 8-13

特定の IP の設定 7-19

リストの設定 7-19

ワーム 7-23

しきい値の調整

結果を定期的に保存 8-11

シグニチャ
 生成 12-22
 シグニチャの生成 12-22
 シグニチャの抽出 12-22
 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
 自動保護モード 9-3, 10-1

す

推奨事項 10-2
 アクティブ化 10-4, 10-7
 受け入れ 10-7
 概要 10-2
 決定の変更 7-22
 コマンド 10-7
 動的フィルタ 10-2
 非アクティブ化 10-4, 10-9
 表示 10-5
 保留フィルタの表示 10-3, 10-6
 無視 10-7
 スーパーバイザ エンジン
 シャットダウン 2-11
 設定 2-1
 設定の確認 2-13
 設定の保存 2-1
 電源の切断 2-11
 ブート 2-12
 リセット 2-11
 スーパーバイザ エンジンの保存
 保存 2-1
 スタティック ルート、追加 3-12
 スプーフィング攻撃 1-4

せ

セッション、アイドル タイムアウトの表示 4-37
 セッション タイムアウト、ディセーブル化 4-37
 セッション、タイムアウトの設定 4-37
 設置、確認 2-2
 設定コマンド 3-8
 設定ファイル
 インポート 13-5
 エクスポート 13-3
 コピー 13-3
 表示 12-3

設定モード
 アクセス 4-12
 説明 3-3

そ

ゾーン
 IP アドレス 5-9
 IP アドレスの削除 5-10
 IP アドレスの除外 5-9
 IP アドレスの定義 5-9
 IP アドレスの変更 5-9
 LINK テンプレート 8-5
 異常検出 9-2
 オフラインでの同期 5-16
 カウンタのクリア 12-6
 コピー 5-6
 コマンド 5-5, 5-6, 10-4
 コマンド補完 4-13, 5-8
 再設定 5-8
 削除 5-6
 作成 5-5
 自動的な同期 5-14
 ステータスの表示 12-4
 設定のエクスポート 5-19
 設定の同期 5-11
 設定の表示 5-8
 設定モード 3-3, 5-8
 テンプレート 5-3
 動作モード 5-6
 比較 8-17
 複製 5-6
 ポリシーの表示 7-26
 ラーニング 8-2

ゾーン同期 8-4

ゾーンのポリシー

調整済みのマーク付け 5-10, 8-13
 ソフトウェア バージョン番号、表示 12-2
 ソフトウェア ライセンス キー、キー情報の表示 12-2
 ゾンビ 1-4

た

帯域幅オプション
 2 Gbps へのアップグレード 13-20

説明 1-9
 ソフトウェア バージョンの表示 12-2
 ソフトウェア ライセンス キーの表示 12-2
 タイムアウトセッション、設定 4-37
 タイムアウトセッション、ディセーブル化 4-37

て

定期的なアクション
 非アクティブ化 8-6, 8-9
 ポリシーの自動受け入れ 8-6, 8-9
 ディセーブル化、自動エクスポート 13-8
 デフォルト設定、~に戻す 13-23
 テンプレート
 LINK 8-5
 ゾーン 5-3
 ポリシーの表示 5-6

と

同期
 設定のエクスポート 13-7
 動的フィルタ 10-2
 1000 以上 6-16
 イベントの表示 12-9
 概要 6-2, 6-15
 コマンド 6-17, 6-18, 9-10
 削除 6-18
 ソート 6-15
 定義 1-7
 ~の作成の防止 6-18
 表示 6-15
 ワーム 7-24
 特定の IP しきい値 7-19
 特権レベル 3-2
 ~の間の移動 4-11
 パスワードの割り当て 4-10
 トラップ 12-11
 トラフィック、監視 12-18
 トラフィックの送信元
 SPAN 2-4
 VACL 2-4
 キャプチャ 2-4
 設定 2-4

に

認可
 zone コマンド補完のディセーブル化 4-13, 5-8
 設定 4-9, 4-10
 認証、設定 4-5
 認証されていない TCP の検出された異常 11-3

ね

ネットワーク サーバ
 sync-config の表示 5-19, 13-8, 13-9
 削除 13-3
 設定 13-2
 表示 13-3, 13-9
 ネットワーク サーバ、設定 13-2

は

バークリー パケット フィルタ 6-8
 バージョン、アップグレード 13-23
 バイパス フィルタ
 コマンド 6-12
 削除 6-14
 設定 6-12
 定義 1-7, 6-2
 表示 6-13
 ハイブリッド 11-6
 パケット、キャプチャ 12-16
 パスワード
 暗号化された 4-7
 イネーブル化 4-10
 復旧 13-23, 13-24
 変更 4-7
 パスワード、復旧 13-24
 バナー、ログインの設定 4-34
 パラメータのリブート 13-9

ひ

非スプーフィング攻撃 1-4

- ふ
- ファイル サーバ
 - sync-config の表示 13-9
 - 設定 13-2
 - ファシリティ 12-11
 - フィルタ
 - 動的 1-7, 6-2, 6-15
 - バイパス 1-7, 6-12
 - フレックスコンテンツ 1-7, 6-3
 - フラッシュの焼き付け 13-18
 - フレックスコンテンツ フィルタ
 - 設定 6-3
 - 定義 1-7, 6-2
 - 番号変更 6-3
 - 表示 6-9
 - フィルタリング基準 6-3
 - フレックスコンテンツ フィルタの番号変更 6-3
 - プロキシ ポリシー テンプレート、プロキシが使用されない場合のポリシー テンプレート 7-5
 - プロキシが使用されない場合のポリシー テンプレート 7-5
- へ
- 返送 IP サマライズ 12-15, 12-16
- ほ
- ポート スキャン 11-6
 - 検出された異常 11-3
 - ポリシー テンプレート 7-4
 - 保護
 - アクティベーション方式 9-4
 - インタラクティブ モード 10-1
 - 自動モード 9-3, 10-1
 - 非アクティブ化 9-5
 - ホスト、ロギング 12-11
 - ホスト鍵
 - 削除 4-21
 - ホスト鍵、削除 4-22
 - ポリシー
 - copy-policies 8-18
 - learning-params fixed-threshold コマンド 7-17
 - threshold-list コマンド 7-19
 - アクション 7-14, 7-20, 7-21
 - アクティブ化 7-15
 - 現在の～のバックアップ 7-30, 8-20
 - 構築 1-6, 8-2, 8-5
 - コマンド 7-14
 - サービスの削除 7-11
 - サービスの追加 7-10
 - しきい値 7-14, 7-17
 - しきい値の乗算 7-18
 - しきい値の調整 1-6, 8-2, 8-8
 - しきい値を固定 7-17
 - 状態 7-15
 - 設定モード 3-3
 - タイムアウト 7-14, 7-20
 - 調整済みのマーク付け 5-10, 8-13
 - ディセーブル化 7-15
 - 統計情報の表示 7-27, 8-10
 - トラフィック特性 7-13
 - ナビゲーションパス 7-14
 - パケット タイプ 7-12
 - パラメータのコピー 8-18
 - 非アクティブ化 7-15
 - ワイルドカードの使用 7-14, 7-26, 7-28
 - ポリシー テンプレート
 - max-services 7-6
 - min-threshold 7-7
 - worm_tcp 7-5
 - 概要 7-3
 - コマンド 7-5, 7-7
 - 状態 7-7
 - 設定コマンド レベル 7-5
 - 設定モード 3-3
 - 同期化のための Guard ポリシー テンプレート 7-4
 - パラメータ 7-5
 - リストの表示 7-5
 - ポリシーの構築 8-5
 - ポリシーのしきい値の調整 8-8
 - 保留 10-2
 - 保留動的フィルタ 10-2
 - 表示 10-3, 10-6
- め
- メモリ消費量 12-28
 - メモリ使用率、異常検出エンジン 12-28, 12-30

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 4-6

新しいへの追加 4-6

削除 4-8

システム ユーザ

Admin 2-10

riverhead 2-10

追加 4-6

特権レベル 3-2, 4-10

特権レベルの割り当て 4-6

ユーザ フィルタ

コマンド 6-3

ユーザによって検出された異常 11-3

ら

ラーニング

policy-construction コマンド 8-5

threshold-tuning コマンド 8-8

概要 8-2

結果の同期 8-4

コマンド 8-6, 8-9

しきい値の調整 8-8

プロセスの終了 8-6, 8-9

ポリシーの構築 8-5

ラーニング パラメータ、表示 8-11

ライセンス

XG アップグレード ライセンスの注文 13-20

キーの生成 13-20

り

リモート Guard

アクティブ化 6-17, 9-6

デフォルト リスト 9-8

保護の終了 9-8, 9-9

リスト 9-9

リストのアクティベーション順序 9-9

リモート Guard リスト

表示 9-8, 9-9

る

ルータ設定モード 3-3

ルーティング テーブル

操作 3-12

表示 3-12

れ

レート

表示 12-5

履歴 12-5

レポート

「攻撃レポート」を参照 11-2

ろ

ロギング、設定の表示 12-11

ロギング パラメータ、設定 12-8

ログ ファイル

エクスポート 12-10, 12-12

クリア 12-13

表示 12-11

ログイン バナー

インポート 4-34

削除 4-35

設定 4-34

ロゴ

WBM からの削除 4-37

WBM への追加 4-36

わ

ワーム

概要 7-23

攻撃の識別 7-24

しきい値 7-23, 7-24

動的フィルタ 7-24

ポリシー 7-12, 7-13

ポリシー テンプレート 7-4, 7-24