CISCO SYSTEMS

Cisco Anomaly Guard Module コンフィギュレーション ガイド

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用

Software Release 5.0
July 2005

Text Part Number: OL-7984-01-J

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。見当たらない場合には、代理店にご連絡ください。

以下の情報は Class A 装置の FCC 適合に関するものです。この装置はテスト済みであり、FCC ルールの Part 15 に記載されている Class A デジタル装置の制限に準拠していることが確認済みです。この制限により、Class A デジタル装置を商業施設で作動させた場合、有害な干渉が起きないようになっています。この装置は、無線周波エネルギーを発生、使用し、また放射することもあります。取り扱い説明書に従って設置または使用しなかった場合には、無線通信に有害な干渉を起こすことがあります。また、この装置を住居で使用する場合には有害な干渉を起こすことがあり、ユーザ側の費用で干渉防止措置を講じなければならない場合があります。

以下の情報は Class B 装置の FCC 適合に関するものです。このマニュアルで解説している装置は、無線周波エネルギーを発生し、また放射することもあります。シスコのインストレーションに関する指示に従って設置されない場合には、ラジオやテレビの受信に干渉を起こす可能性があります。この装置は、テスト済みであり、FCC ルールの Part 15 に記載されている仕様に基づく Class B デジタル装置の制限に準拠していることが確認済みです。この仕様では、住居に設置した場合にこのような干渉が起きないようになっています。ただし、特定の設置条件で干渉が起きないことを保証するものではありません。

シスコによる書面での認可なしに装置に対して変更を行うと、Class A または Class B デジタル装置に要求される FCC への適合ができない可能性があります。この場合、装置の使用権限は FCC 規制によって制限され、ユーザ側の費用でラジオまたはテレビへの干渉防止措置を講じなければならない場合があります。

装置の電源を切ることによって、装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコの装置またはその周辺装置が原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

• 干渉がなくなるまでテレビまたはラジオのアンテナの向きを変えます。

• テレビまたはラジオの左右どちらかの側に装置を移動します。

• テレビまたはラジオから離れた場所に装置を移動します。

• テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビ / ラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

シスコより認められていない変更をこの製品に対して行った場合には、FCC 認定が無効になり、さらに製品を操作するユーザの権限を失うことになります。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。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、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、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、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、および iQuick Study は、Cisco Systems, Inc. のサービス マークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、*Packet*、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、TeleRouter、The Fastest Way to Increase Your Internet Quotient、および TransPath は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルまたは Web サイトで言及されているその他の商標はすべて、それぞれの所有者のものです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。（0502R）

Cisco Anomaly Guard Module コンフィギュレーション ガイド
Copyright © 2005 Cisco Systems, Inc.
All rights reserved.

CONTENTS

このマニュアルについて xxv

対象読者 xxvi

マニュアルの構成 xxvii

表記法 xxviii

技術情報の入手方法 xxx

Cisco.com xxx

Product Documentation DVD（英語版） xxx

マニュアルの発注方法（英語版） xxxi

シスコシステムズマニュアルセンター xxxii

シスコ製品のセキュリティの概要 xxxiii

シスコ製品のセキュリティ問題の報告 xxxiii

テクニカル サポート xxxv

Cisco Technical Support & Documentation Web サイト xxxv

Japan TAC Web サイト xxxvi

サービス リクエストの発行 xxxvi

サービス リクエストのシビラティの定義 xxxvii

その他の資料および情報の入手方法 xxxviii

CHAPTER 1 概要 1-1

DDos について 1-2

Cisco Anomaly Guard Module 1-3

ゾーンについて 1-4
Guard モジュールの動作のしくみについて 1-5
保護のメカニズム 1-8
フィルタ 1-8
保護モジュール 1-9
保護サイクル 1-10

CHAPTER 2 スーパーバイザ エンジンへの Guard モジュールの設定 2-1
Guard モジュールの設置の確認 2-3
Guard モジュールの管理の設定 2-5
VLAN の設定 2-6
スーパーバイザ エンジンへの VLAN の設定 2-6
Guard モジュールへの VLAN の割り当て 2-7
VLAN へのレイヤ 3 インターフェイスの設定 2-8
Guard モジュールとのセッションの確立 2-9
Guard モジュールのリブート 2-11
Guard モジュールの設定の確認 2-13
1 つのスイッチに対する複数の Guard モジュールの設定 2-14
ロード シェアリング 2-14
冗長性と高いアベイラビリティ 2-15

CHAPTER 3 Guard モジュールの初期化 3-1
コマンドライン インターフェイスの使用 3-2
CLI でのコマンドの発行 3-3
コマンドの no 形の使用 3-5
show コマンドの構文 3-5
CLI のエラー メッセージ 3-5

CLI 使用のヒント 3-6
ヘルプ 3-6
タブ補完 3-6
操作の方向の規定 3-7
コマンドの省略 3-7
ワイルドカード文字 3-7
Guard モジュールのインターフェイスの設定 3-8
物理インターフェイスの設定 3-9
VLAN の設定 3-11
ループバック インターフェイスの設定 3-12
デフォルト ゲートウェイの設定 3-14
ルーティング テーブルへのスタティック ルートの追加 3-15
プロキシ IP アドレスの設定 3-17
Guard モジュールの管理 3-18
Web ベース管理による Guard モジュールの管理 3-18
SSH を使用した Guard モジュールへのアクセス 3-19

CHAPTER 4 Guard モジュールの設定 4-1
Guard モジュールのサービスのアクティブ化 4-2
アクセス コントロールの設定：認証、認可、アカウンティングの使用 4-5
認証の設定 4-6
認証方式の設定 4-7
ローカル認証の設定 4-8
認可の設定 4-11
ローカル許可の設定 4-12
認可方式の設定 4-14

アカウンティングの設定 4-17
TACACS+ サーバのアトリビュートの設定 4-18
TACACS+ サーバの IP アドレスの設定 4-19
TACACS+ サーバの暗号鍵の設定 4-20
TACACS+ の検索の設定 4-20
TACACS+ サーバの接続タイムアウトの設定 4-21
TACACS+ サーバの統計情報の表示 4-22
Cisco Traffic Anomaly Detector Module との通信のイネーブル化 4-23
SSL 通信チャネルの設定 4-24
SSL 通信チャネルの確立 4-24
SSL 証明書の再生成 4-26
SSH 通信チャネルの設定 4-27
SSH 通信チャネルの確立 4-28
SSH 通信チャネル鍵の再生成 4-28
日付と時刻の設定 4-30
SSH 鍵の管理 4-31
SSH 鍵の追加 4-31
SSH 鍵の削除 4-32
SFTP 接続の鍵の設定 4-33
ホスト名の変更 4-35
SNMP トラップのイネーブル化 4-36
SNMP コミュニティ ストリングの設定 4-38

CHAPTER 5 トラフィックの宛先変更の設定 5-1
概要 5-2
トラフィックの宛先変更 5-3

ネットワーク設定 5-3
宛先変更のメカニズム 5-5
ハイジャック パラメータ 5-7
注入パラメータ 5-8
宛先変更ルートの表示 5-9
インライン ネットワーク設定 5-11
ハイジャック 5-11
注入 5-11
インラインの宛先変更の設定 5-12
アウトオブパス ネットワーク設定 5-16
ハイジャック 5-16
注入 5-17
アウトオブパスの宛先変更の設定 5-17
トラフィック注入方式 5-23
レイヤ 2 トポロジ 5-23
レイヤ 3 トポロジ 5-23
VRF の設定 5-25

CHAPTER 6 ゾーンの設定 6-1
概要 6-2
ゾーンの作成 6-3
新しいゾーンの作成 6-4
ゾーンの複製 6-7
ゾーンのアトリビュートの設定 6-9
ゾーン トラフィックの特性のラーニング 6-13
ラーニング プロセスの概要 6-13

ゾーンのラーニング プロセスの結果と Cisco Traffic Anomaly Detector Module の同期 6-16
ポリシーの構築 6-17
しきい値の調整 6-19
ラーニング パラメータの設定 6-24
定期的なアクションの設定 6-25
しきい値選択方式の設定 6-26
ポリシーへの調整済みのマーク付け 6-27
ゾーン ポリシーのしきい値の調整とゾーン保護のイネーブル化の同時実行 6-29
Guard モジュールのゾーン設定と Detector モジュールの同期 6-30
設定のガイドライン 6-30
サンプル シナリオ 6-31
オフラインでのゾーン設定の同期 6-33
ゾーンの保護 6-35
ゾーン保護のアクティブ化 6-36
ゾーン保護の非アクティブ化 6-38
保護動作モードの定義 6-38
アクティベーション方式の設定 6-39
アクティベーション範囲の設定 6-41
サブゾーンについて 6-42
保護の無活動タイムアウトの設定 6-43
オンデマンド保護のイネーブル化 6-45

CHAPTER 7 ゾーンのフィルタの設定 7-1
概要 7-2
フィルタのトラフィック フロー 7-4

フレックスコンテンツ フィルタの設定 7-7
フレックスコンテンツ フィルタの追加 7-8
TCPDump 式の構文について 7-13
パターン式の構文について 7-16
フレックスコンテンツ フィルタの表示 7-18
フレックスコンテンツ フィルタの削除 7-19
フレックスコンテンツ フィルタの状態の変更 7-20
バイパス フィルタの設定 7-21
バイパス フィルタの追加 7-21
バイパス フィルタの表示 7-22
バイパス フィルタの削除 7-23
ユーザ フィルタの設定 7-24
ユーザ フィルタの追加 7-26
ユーザ フィルタの表示 7-28
ユーザ フィルタの削除 7-29
動的フィルタの設定 7-31
動的フィルタの追加 7-33
動的フィルタの表示 7-34
動的フィルタの削除 7-37
動的フィルタの非アクティブ化 7-38

CHAPTER 8 ポリシー テンプレートとポリシーの設定 8-1
ポリシーについて 8-2
ポリシー パス構造 8-2
ポリシーの作成 8-4
ポリシー テンプレートについて 8-5
ポリシー テンプレート パラメータの設定 8-8

サービスの最大数の設定 8-9
最小しきい値の設定 8-11
ポリシー テンプレートの状態の設定 8-11
すべてのポリシー テンプレート パラメータの同時設定 8-12
ポリシー パスのセクションについて 8-14
サービス 8-14
サービスの追加 8-15
サービスの削除 8-16
保護モジュール 8-18
パケット タイプ 8-18
トラフィック特性 8-20
ポリシー パラメータの設定 8-21
ポリシーの状態の変更 8-22
ポリシーのしきい値の設定 8-23
ポリシーのしきい値の設定 8-24
固定値としてのしきい値の設定 8-25
しきい値の乗数の設定 8-26
係数によるしきい値の乗算 8-27
特定の IP しきい値の設定 8-28
プロキシしきい値の設定 8-29
ポリシーのタイムアウトの設定 8-30
ポリシーのアクションの設定 8-31
ポリシーのインタラクティブ ステータスの設定 8-32
ポリシーの監視 8-34
ポリシーの表示 8-34
ポリシーの統計情報の表示 8-36

スナップショットを使用したラーニング プロセスの結果の確認 8-38
スナップショットの作成 8-38
ラーニングの結果の比較 8-40
スナップショットの比較 8-41
ゾーンの比較 8-42
スナップショットの表示 8-42
ポリシーのコピー 8-44

CHAPTER 9 インタラクティブ保護モード 9-1
概要 9-2
インタラクティブ保護モードのアクティブ化 9-4
インタラクティブ保護モードの非アクティブ化 9-4
推奨事項の表示 9-5
推奨事項の管理 9-9

CHAPTER 10 攻撃レポート 10-1
レポートのレイアウトについて 10-2
General Details 10-3
Attack Statistics 10-3
Dropped/ Replied Packets 10-4
Detected Anomalies 10-5
Mitigated Attacks 10-6
スプーフィング利用 10-7
ゾンビ 10-8
クライアント攻撃 10-9
ユーザ定義 10-10

不正な形式のパケット 10-11
Zombies 10-11
レポートのパラメータについて 10-12
攻撃レポートの表示 10-14
攻撃レポートのエクスポート 10-19
攻撃レポートの自動エクスポート 10-19
すべてのゾーンの攻撃レポートのエクスポート 10-20
ゾーン レポートのエクスポート 10-22

CHAPTER 11 Guard モジュールの診断ツールの使用方法 11-1
Guard モジュールの設定の表示 11-2
Guard モジュールのゾーンの表示 11-3
ゾーンのカウンタの表示 11-4
ゾーンのステータスの表示 11-6
Guard モジュールのログの表示 11-7
オンライン イベント ログの表示 11-8
オンライン イベント ログのエクスポート 11-8
ログ ファイルの表示 11-11
ログ ファイルのエクスポート 11-11
ログ ファイルのクリア 11-12
ネットワーク トラフィックの監視および攻撃のシグニチャの抽出 11-14
Guard モジュールの設定によるトラフィックの自動記録 11-16
Guard モジュールのアクティブ化によるトラフィックの手動記録 11-18
Guard モジュールによるトラフィックの手動記録の停止 11-21

手動パケットダンプ設定の表示 11-21
パケットダンプ キャプチャ ファイルの自動エクスポート 11-22
パケットダンプ キャプチャ ファイルの手動エクスポート 11-23
パケットダンプ キャプチャ ファイルのインポート 11-25
パケットダンプ キャプチャ ファイルの表示 11-27
パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成 11-28
パケットダンプ キャプチャ ファイルのコピー 11-31
パケットダンプ キャプチャ ファイルの削除 11-32
一般的な診断データの表示 11-34
メモリ消費量の表示 11-35
CPU 使用率の表示 11-36
ARP キャッシュの操作 11-37
netstat の使用 11-40
traceroute の使用 11-43
ping の使用 11-45
デバッグ情報の取得 11-47
Guard モジュールの自己保護設定の表示 11-49
フレックスコンテンツ フィルタのデフォルト設定 11-49

CHAPTER 12 メンテナンス タスクの実行 12-1
設定のエクスポート 12-2
設定のインポートとアップデート 12-4
Guard モジュールのリロード 12-7
Guard モジュールのリブート 12-7
Guard モジュールのバージョンのアップグレード 12-8

アップグレード時の注意事項 12-9
AP のアップグレード手順 12-11
MP のアップグレード手順 12-14
インライン アップグレード手順 12-17
新しいフラッシュ バージョンの焼き付け 12-21
MP 関連のコマンド 12-23
忘失パスワードの復旧 12-24
工場出荷時のデフォルト設定へのリセット 12-25

CHAPTER 13 Guard モジュールによる軽減の分析 13-1
ゾーンのトラフィック パターンの分析 13-2
宛先変更の問題 13-3
フロー特性に基づくゾーンへのフローのブロッキング 13-3
トラフィック ブロッキング基準の確認 13-5
攻撃の軽減の確認 13-8
ゾーンの現在の攻撃レポートの表示 13-8
Guard モジュールの高度な統計情報の表示 13-9
ドロップされたトラフィックの統計情報の表示 13-10

INDEX 索引

FIGURES

図 1-1 Cisco Anomaly Guard Module **の動作** **1-5**

図 1-2 Guard **の保護サイクル** **1-10**

図 5-1 **インライン ネットワーク設定** **5-4**

図 5-2 **アウトオブパス ネットワーク設定** **5-5**

図 5-3 **宛先変更のメカニズム** **5-6**

図 5-4 **インライン ネットワーク設定（**L3 **トポロジ）の例** **5-12**

図 5-5 **アウトオブパス ネットワーク設定（**L3 **トポロジ）の例** **5-18**

図 5-6 **レイヤ** 3 **注入の設定例** **5-25**

図 7-1 Guard **モジュールのフィルタ システム** **7-3**

図 8-1 **ポリシー名** **8-3**

TABLES

表 2-1 anomaly-guard **コマンドの引数** **2-5**
表 2-2 anomaly-guard module **コマンドの引数** **2-7**
表 2-3 session slot **コマンドの引数** **2-9**
表 2-4 show module **コマンドの引数** **2-13**
表 3-1 **ユーザの特権レベル** **3-2**
表 3-2 CLI **の規則** **3-3**
表 3-3 speed **コマンドの引数とキーワード** **3-10**
表 3-4 ip route **コマンドの引数** **3-15**
表 4-1 Guard **モジュール サービス** **4-2**
表 4-2 permit **コマンドの引数** **4-4**
表 4-3 aaa authentication **コマンドのキーワード** **4-7**
表 4-4 username **コマンドの引数とキーワード** **4-9**
表 4-5 enable password **コマンドの引数** **4-13**
表 4-6 aaa authorization **コマンドの引数とキーワード** **4-15**
表 4-7 aaa accounting **コマンドのキーワード** **4-17**
表 4-8 show tacacs statistics **コマンド出力のフィールドの説明** **4-22**
表 4-9 date **コマンドの引数** **4-30**
表 4-10 key add **コマンドの引数とキーワード** **4-31**
表 4-11 key remove **コマンドの引数** **4-32**
表 4-12 snmp trap-dest **コマンドの引数** **4-36**
表 5-1 diversion hijacking **コマンドの引数** **5-8**
表 6-1 zone **コマンドの引数とキーワード** **6-4**
表 6-2 **ゾーン テンプレート** **6-5**
表 6-3 zone **コマンドの引数** **6-7**
表 6-4 ip address **コマンドの引数** **6-9**

表 6-5 rate limit コマンドの引数 6-11
表 6-6 learning-params periodic-action コマンドの引数とキーワード 6-25
表 6-7 learning-params threshold-selection コマンドの引数とキーワード 6-26
表 6-8 protection-end-timer コマンドの引数とキーワード 6-43
表 7-1 フィルタのフローの引数 7-4
表 7-2 フィルタの show コマンドのフィールドの説明 7-6
表 7-3 flex-filter renumber コマンドの引数 7-8
表 7-4 flex-filter コマンドの引数とキーワード 7-9
表 7-5 フレックスコンテンツ フィルタのパラメータ 7-13
表 7-6 フレックスコンテンツ フィルタの式の規則 7-14
表 7-7 フレックスコンテンツ パターン フィールドの説明 7-17
表 7-8 show flex-content-filters コマンドのフィールドの説明 7-18
表 7-9 bypass-filter コマンドの引数 7-22
表 7-10 show bypass-filters コマンドのフィールドの説明 7-22
表 7-11 ユーザ フィルタのアクション 7-25
表 7-12 user-filter renumber コマンドの引数 7-26
表 7-13 user-filter コマンドの引数とキーワード 7-27
表 7-14 show コマンドにおけるユーザ フィルタのフィールドの説明 7-28
表 7-15 動的フィルタのアクション 7-32
表 7-16 dynamic-filter コマンドの引数とキーワード 7-33
表 7-17 show dynamic-filters コマンドの引数 7-35
表 7-18 show dynamic-filters コマンド出力のフィールドの説明 7-36
表 7-19 show dynamic-filters details コマンドのフィールドの説明 7-36
表 8-1 ポリシー名のセクション 8-3
表 8-2 ポリシー テンプレート 8-5
表 8-3 GUARD_TCP_NO_PROXY のポリシー テンプレート 8-8
表 8-4 policy-template コマンドの引数とキーワード 8-12
表 8-5 policy-template コマンドの引数 8-16
表 8-6 remove-service コマンドの引数 8-17
表 8-7 パケット タイプ 8-19
表 8-8 トラフィック特性 8-20

表 8-9 learning-params threshold-multiplier **コマンドの引数** **8-26**
表 8-10 policy thresh-mult **コマンドの引数** **8-27**
表 8-11 policy threshold-list **コマンドの引数** **8-28**
表 8-12 timeout **コマンドの引数とキーワード** **8-30**
表 8-13 **ポリシーのアクション** **8-31**
表 8-14 interactive-status **コマンドのキーワード** **8-33**
表 8-15 show policies **コマンド出力のフィールド説明** **8-35**
表 8-16 show policies statistics **コマンドの引数** **8-36**
表 8-17 show policies statistics **コマンド出力テーブルのフィールド説明** **8-37**
表 8-18 snapshot **コマンドの引数とキーワード** **8-39**
表 8-19 diff **コマンドの引数** **8-41**
表 8-20 diff **コマンドの引数** **8-42**
表 8-21 show snapshots **コマンドの引数とキーワード** **8-43**
表 8-22 show snapshots **コマンド出力のフィールドの説明** **8-43**
表 8-23 copy-policies **コマンドの引数とキーワード** **8-44**
表 9-1 show recommendations **コマンドのキーワードと引数** **9-5**
表 9-2 show recommendations **コマンドのフィールド説明** **9-6**
表 9-3 show recommendations pending-filters **コマンドのフィールド説明** **9-7**
表 9-4 recommendation **コマンドの引数とキーワード** **9-10**
表 10-1 **攻撃レポートの** General Details **セクションのフィールド説明** **10-3**
表 10-2 **パケット タイプ** **10-3**
表 10-3 **ドロップされたパケットおよび返送されたパケットのタイプ** **10-4**
表 10-4 **検出された異常のタイプ** **10-5**
表 10-5 **スプーフィングを利用した攻撃のタイプ** **10-7**
表 10-6 **ゾンビ攻撃のタイプ** **10-8**
表 10-7 **クライアント攻撃のタイプ** **10-9**
表 10-8 **ユーザ定義攻撃のタイプ** **10-10**
表 10-9 **不正形式パケットのタイプ** **10-11**
表 10-10 Attack Statistics **のフィールド説明** **10-12**
表 10-11 **フロー統計情報のフィールド説明** **10-12**
表 10-12 show reports **コマンドの引数とキーワード** **10-14**

表 10-13 show reports **コマンド出力のフィールドの説明** **10-15**
表 10-14 **詳細なレポートのフローのフィールド説明** **10-17**
表 10-15 **ゾンビ攻撃に関するテーブルのフィールドの説明** **10-18**
表 10-16 export reports **コマンドの引数** **10-20**
表 10-17 copy reports **コマンドの引数とキーワード** **10-21**
表 10-18 copy zone reports **コマンドの引数とキーワード** **10-22**
表 11-1 show running-config **コマンドのキーワード** **11-2**
表 11-2 **ゾーンのステータス** **11-3**
表 11-3 Guard **モジュールのカウンタ** **11-5**
表 11-4 **イベント ログのレベル** **11-7**
表 11-5 logging **コマンドのキーワード** **11-9**
表 11-6 copy log ftp **コマンドの引数** **11-12**
表 11-7 **自動パケットダンプ キャプチャ ファイル名のセクション** **11-16**
表 11-8 packet-dump **コマンドの引数とキーワード** **11-19**
表 11-9 **手動の** show packet-dump **コマンド出力のフィールドの説明** **11-22**
表 11-10 export packet-dump **コマンドの引数** **11-23**
表 11-11 copy zone packet-dump **コマンドの引数とキーワード** **11-24**
表 11-12 copy zone packet-dump **コマンドの引数** **11-26**
表 11-13 show packet-dump captures **コマンドの引数** **11-27**
表 11-14 show packet-dump captures **コマンド出力のフィールドの説明** **11-28**
表 11-15 show packet-dump signatures **コマンドの引数** **11-29**
表 11-16 show packet-dump signatures **コマンド出力のフィールドの説明** **11-30**
表 11-17 copy packet-dump captures **コマンドの引数** **11-31**
表 11-18 clear packet-dump **コマンドの引数** **11-33**
表 11-19 arp **コマンドの引数とキーワード** **11-37**
表 11-20 netstat **コマンドの引数とキーワード** **11-41**
表 11-21 traceroute **コマンドの引数とキーワード** **11-43**
表 11-22 ping **コマンドの引数とキーワード** **11-45**
表 11-23 copy debug-core **コマンドの引数** **11-48**
表 11-24 **フレックスコンテンツ フィルタのデフォルト設定** **11-50**
表 12-1 copy running-config ftp **コマンドの引数** **12-2**

表 12-2 copy ftp running-config **コマンドの引数** **12-5**
表 12-3 MP **関連のコマンド** **12-23**
表 13-1 **ドロップ統計情報** **13-10**

このマニュアルについて

このマニュアルでは、Cisco Anomaly Guard Module（Guard モジュール）について説明します。具体的には、管理作業の実行方法、Guard の運用に必要となる一般的な操作の方法、および Guard モジュールの使用方法を示します。

ここでは、このマニュアルの対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

この章には、次の項があります。

- 対象読者
- マニュアルの構成
- 表記法
- 技術情報の入手方法
- シスコ製品のセキュリティの概要
- テクニカル サポート
- その他の資料および情報の入手方法

対象読者

『*Cisco Anomaly Guard Module コンフィギュレーション ガイド*』は、次の方を対象としています。

- ネットワーク管理者
- エンジニア
- オペレータ
- ネットワーク セキュリティの専門家

このマニュアルでは、ネットワーキングおよびネットワーク セキュリティに関する幅広い知識を前提としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章番号	説明
第 1 章「概要」	Cisco Anomaly Guard Module（Guard モジュール）の概要を示し、Guard モジュールの動作状態およびコンポーネントについて概説します。
第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」	Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに Guard モジュールを設定する方法について説明します。
第 3 章「Guard モジュールの初期化」	Guard モジュールを接続し、設定するために必要な最初の手順について説明します。また、Guard モジュールの CLI 環境および認証方法を概説します。
第 4 章「Guard モジュールの設定」	Guard モジュールのサービスとアクセス コントロールを設定する方法について説明します。
第 5 章「トラフィックの宛先変更の設定」	ゾーンのトラフィックの宛先変更プロセスについて説明し、宛先変更を設定する方法を詳しく示します。
第 6 章「ゾーンの設定」	ゾーンの作成方法および管理方法について説明します。
第 7 章「ゾーンのフィルタの設定」	Guard モジュールのフィルタについて説明し、フィルタを設定する方法を詳しく示します。
第 8 章「ポリシー テンプレートとポリシーの設定」	Guard モジュールのポリシーおよびポリシー テンプレートについて説明し、これらを設定する方法を詳しく示します。
第 9 章「インタラクティブ保護モード」	インタラクティブ保護モードについて説明します。また、Guard モジュールの推奨事項、ユーザの決定に関するオプション、およびポリシーのインタラクティブ ステータスについて説明します。
第 10 章「攻撃レポート」	Guard モジュールの攻撃レポート、レポートの構成、およびオプションの表示について説明します。
第 11 章「Guard モジュールの診断ツールの使用方法」	Guard モジュールの診断ツールについて説明します。
第 12 章「メンテナンス タスクの実行」	Guard モジュールのメンテナンスおよび管理に必要な作業を実施する方法について説明します。
第 13 章「Guard モジュールによる軽減の分析」	ゾーンのトラフィック パターンを分析する方法について説明し、設定上の問題を特定します。また、攻撃のタイプを特定する方法と、分析に基づいた推奨アクションを簡単に示します。

表記法

このマニュアルは、次の表記法を使用しています。

スタイルまたは記号	説明
太字	太字のテキストを記載されているとおりに入力します。コマンドおよびキーワードは、太字 で示しています。
イタリック体	ユーザが値を指定する変数を示します。
標準スタイルのテキスト	プロンプトなどの画面表示を表します。標準スタイルのテキストをコマンドの一部として入力しないでください。
[x]	角カッコの中のキーワードは、省略可能です。
[x | y]	角カッコの中のキーワードが縦棒で区切られている場合は、省略可能なキーワードを複数の値の中から 1 つ選択することを示します。
{x | y | z}	必須キーワードの選択肢は、波カッコで囲まれ、縦棒で区切られています。必ず 1 つ選択する必要があります。
[x {y | z}]	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。必ずしもどれか 1 つを選択する必要はありません。選択する場合は、指定された選択肢の中から選びます。

このマニュアルでは、例としてゾーン名に *scannet*、プロンプトに *user@GUARD-conf-zone-scannet#* を使用しています。

このマニュアルでは、さまざまな種類の情報を区別するために次の記号と表記法を使用しています。

注意 注意は、ユーザによる特定の操作が、データ損失または機器への悪影響につながる可能性があることを意味します。

警告　**警告は、人身事故または機器の損傷につながる可能性のある操作を表します。**

（注）　「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント　ここに記載されている情報が、問題の解決に役立つことを意味します。ヒントの情報はトラブルシューティングや対策にはなりませんが、情報として役立てることができます。

ワンポイント・アドバイス　時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカル サポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

最新のシスコのマニュアルには、次の URL からアクセスしてください。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

各国のシスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering Tool または Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

Cisco Ordering Tool：

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace：

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Ordering Tool を使用したマニュアル発注も引き続きご利用いただけます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering Tool から英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/
- Ordering Tool を使用した英文マニュアル発注の手順については、次の URL を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

概要

この章では、Cisco Anomaly Guard Module（Guard）の概要、コンポーネント、および動作のしくみについて説明します。この章には、次の項があります。

- DDos について
- Cisco Anomaly Guard Module
- ゾーンについて
- Guard モジュールの動作のしくみについて
- 保護のメカニズム
- 保護サイクル

DDos について

Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃は、悪意のある個人が、セキュリティを侵された数千台ものコンピュータ（ゾンビ）に自動化されたスクリプトを実行させて偽のサービス要求を発行し、保護されたサーバ（ゾーン）のネットワーク リソースを使用不能にする攻撃です。このような攻撃には、Web サーバに偽のホームページ要求を大量に送信して正当な消費者がアクセスできないようにしたり、Domain Name System（DNS; ドメイン ネーム システム）サーバのアベイラビリティと正確性を低下させようとしたりするものなどがあります。ゾンビは、多くの場合、個人によって開始されますが、実際に攻撃用コードを実行しているものは、複数の組織によって管理される複数の自律システム上に分散しており、その数は何十万にも及ぶ可能性があります。このような分散攻撃は、大企業も含めた一般的なゾーンで使用される低い帯域幅では処理できない大量のトラフィックを発生させます。

DDoS 攻撃は統計的な現象であるため、詳細で統計的なトラフィック プロファイルの形成が必要になります。DDoS の調査では、DDoS のゾンビは自律システム内に多数分散していること、正当なサービス要求と偽のサービス要求が密に統合されていること、および、DDoS 攻撃ではランダムな設定（IP 送信元アドレスのスプーフィングや TCP フラグのランダム設定など）が使用されていることなどが指摘されています。

高度な知識を持ったハッカーは、攻撃用の新たな不正手段を生み出し続けており、DDoS 攻撃は常に進化しています。また、これらの攻撃スクリプトはインターネット上で容易に入手でき、ネットワークに関する技術知識があまりない人物がごく普通に実行しています。このため、DDoS 防御テクノロジーは柔軟かつ臨機応変なものである必要があります。

つまり、DDoS 防御システムは、近づく DDoS 攻撃を検出し、悪意のあるトラフィックと正常なトラフィックを区別し、攻撃対象となっているネットワーク要素のトラフィック フローを妨げることなくこれらのタスクを実行できるものである必要があります。

Cisco Anomaly Guard Module

Cisco Anomaly Guard Module（Guard モジュール）は Cisco IOS アプリケーション モジュールの 1 つで、次の製品のどちらかに設置できます。

- Supervisor Engine 720（SUP720）、または Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を備えた Supervisor Engine 2（SUP2）が搭載された、Cisco Catalyst 6500 シリーズ スイッチ
- SUP720 が搭載された Cisco 7600 ルータ

このサービス拒絶（DoS）軽減製品は、攻撃対象から宛先変更されたトラフィックを受信して特定の攻撃パケットを識別して削除し、正当なトラフィックを元の宛先に転送します。この製品は、分散型のアップストリーム構成に ISP、MSP、またはバックボーン レベルで導入され、ネットワーク全体を保護します。攻撃が検出されると、攻撃対象ゾーンのトラフィックのみが宛先変更され、Guard に送られます。また、データ フローが分析されます。すべての DDoS コンポーネントは除去され、クリーンなトラフィックが継続して目的のゾーンへ流されます。Guard は、トラフィックを常時フィルタリングしながらゾーンの透過的なトラフィック フローを可能にし、新たに発生する攻撃パターンに備えるために、常にゾーンのトラフィック特性に合せて調整された状態を保ちます。

このような動作を行うために、Guard では、次のコンポーネントが使用されています。

- トラフィックの宛先変更メカニズム。このメカニズムにより、ゾーンのトラフィックが Guard のラーニング システムと保護システムにリダイレクト（宛先変更）され、その後正当なトラフィック フローがゾーンに戻され（注入され）ます。この処理は、ネットワーク トラフィックを妨げることなく実行されます。
- アルゴリズムに基づいたラーニング システム。このラーニング システムは、ゾーンのトラフィックをラーニングし、それ自体を特定の特性に適合させ、しきい値とポリシーという形で参考値と保護のための指示を与えることにより、保護システムをサポートします。また、Guard には、Guard がゾーンのトラフィックのラーニング プロセスとそのトラフィックに合せた調整を完了していないときにゾーンが攻撃された場合に対応するために、オンデマンドの保護も用意されています。
- 正当なトラフィックと疑わしいトラフィックを区別し、悪意のあるトラフィックをフィルタリングする保護システム。フィルタリング後は、正当なトラフィックのみがゾーンに渡されます。

Guard は、これらのコンポーネントを統合することにより、攻撃時には保護の役割を果たし、それ以外のときにはバックグラウンドに控えた状態を保つことができます。攻撃の疑いがない場合は、宛先変更プロセスをアクティブにする必要はなく、Guard モジュールはトラフィックを監視しません。

ゾーンについて

ゾーンは、Guard モジュールが DDoS 攻撃からの保護対象とするネットワーク要素です。

ゾーンは、ネットワーク サーバ、クライアント、ルータ、ネットワーク リンク、サブネット、ネットワーク全体、個々のインターネット ユーザ、企業、インターネット サービス プロバイダー（ISP）、またはこれらを組み合せたものを包含できます。

Guard モジュールは、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンを同時に保護できます。

Guard モジュールは、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンのトラフィックを同時に分析できます。

ゾーンはネットワーク要素の定義で、Guard モジュールはこの設定されたゾーンを DDoS 攻撃から保護することができます。

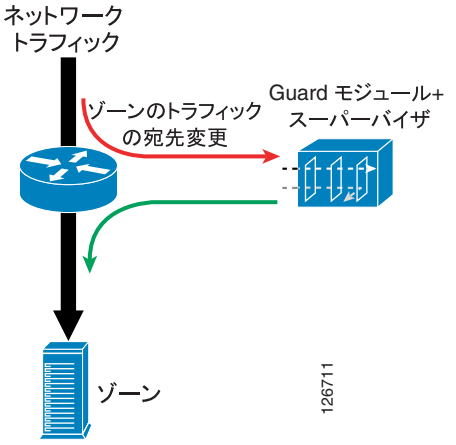
この定義は、ネットワーク アドレスや検出ポリシーなどの設定で構成されます。ゾーンに名前を割り当てて、この名前でゾーンを参照することができます。

Guard モジュールの動作のしくみについて

ターゲット ホスト（ゾーン）を保護するには、そのホストへのトラフィックが宛先変更され、Guard モジュールに送られる必要があります。外部（Cisco Traffic Anomaly Detector Module やその他の手段）から攻撃の兆候が示されてから Guard を設定してゾーンを保護することも、ゾーンの設定完了後すぐにゾーンを保護するように Guard に指示することもできます。Guard は、データ フローを分析します。すべての DDoS 要素はブロックされ、宛先変更されたストリームから悪意のあるパケットが除去されます。クリーンなトラフィックはメインのデータ パスに戻され、目的のゾーンに継続して流されます。図 1-1 に、保護動作の概要を示します。

宛先変更は、Guard モジュールのルーティング設定を通じてグローバルに設定されます。詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

図 1-1　Cisco Anomaly Guard Module の動作



ゾーンのトラフィックを比較する際の基準を作り、悪意の攻撃となる可能性のあるあらゆる異常をトレースするために、Guard はゾーンのトラフィックの特性をラーニングします。

また、ゾーンが攻撃にさらされている場合などは、必要に応じて、ラーニング プロセスを実行せずにゾーンを保護することもできます。システム定義のゾーン テンプレートには、ラーニング プロセスが完了していないゾーンの保護に適した定義済みの保護ポリシーとフィルタが含まれています。詳細については、P.6-45 の「オンデマンド保護のイネーブル化」を参照してください。

ラーニング プロセスは次の 2 つのフェーズで構成されます。これらのフェーズで Guard はゾーンのトラフィックをラーニングし、特定の特性に対応します。

1. **ポリシー構築フェーズ**：ゾーンのポリシーを作成します。ポリシー テンプレートは、ポリシーの構築に使用される規則を提供します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービスを検出できます。
2. **しきい値調整フェーズ**：ゾーンのサービスのトラフィック レートに合せてポリシーを調整します。トラフィック フローは Guard をそのまま通過し、Guard はポリシー構築フェーズで検出されたサービスに使用するしきい値を調整します。

しきい値調整フェーズをアクティブにし、さらにゾーン保護も同時にアクティブにすることができます。この動作状態では、Guard モジュールは、ゾーン ポリシーのしきい値をラーニングし、同時にトラフィックの異常に関するポリシーのしきい値を監視することができます。Guard モジュールは攻撃を検出すると、ラーニング プロセスを停止しますが、ゾーン保護は継続します。この結果、Guard モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。攻撃が終了すると、Guard モジュールはラーニング プロセスを再開します。

ポリシーは、Guard モジュール統計エンジンの構成要素です。各ゾーンには、ゾーンのトラフィック パターンに合せて調整されたポリシーのセットがあります。これらのポリシーは、悪意となる可能性のある異常をトレースするために、Guard モジュールがゾーンのトラフィックと比較する基礎となります。ポリシーは、トラフィック フローを持続的に測定し、特定のトラフィック フローが悪意のあるものまたは異常であると判断すると、そのフローに対してアクションを実行します。このアクションは、フローがポリシーのしきい値を超過すると発生します。

トラフィックのラーニングの詳細については、第 6 章「ゾーンの設定」を参照してください。ゾーンのポリシーの詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください。

トラフィック フローがポリシーのしきい値を超過すると、Guard はそのトラフィックを悪意のあるものまたは異常であると識別します。そして一連のフィルタ（動的フィルタ）を動的に設定し、そのトラフィックを攻撃の重大度に従って適切な保護モジュールに誘導します。

Guard の保護は、次の方法でアクティブにできます。

- 自動保護モード：動的フィルタはユーザの操作なしでアクティブになります。
- インタラクティブ保護モード：動的フィルタは、手動でインタラクティブにアクティブになります。動的フィルタは推奨事項としてグループ化され、ユーザの決定を待ちます。ユーザは、これらの推奨事項を確認して、どの推奨事項を受け入れるか、無視するか、自動アクティベーションに切り替えるかを決定できます。

詳細については、第 9 章「インタラクティブ保護モード」を参照してください。

Guard は、ゾーンのステータスを明確につかめるようにするために、すべてのゾーンの攻撃レポートを提供します。攻撃レポートでは、最初の動的フィルタの生成から保護の終了まで、攻撃の詳細な情報が提供されます。

詳細については、第 10 章「攻撃レポート」を参照してください。

保護のメカニズム

Guard の保護システムでは、次のメカニズムが使用されます。

- フィルタ
- 保護モジュール

フィルタ

ゾーンのフィルタは、宛先変更されたトラフィックを関連する保護モジュールに誘導します。Guard では、ユーザがフィルタを設定して、カスタマイズされたトラフィック誘導や DDoS 攻撃の防止メカニズムをさまざまに設計できるようになっています。Guard では、次のタイプのフィルタが使用されます。

- ユーザ フィルタ：指定されたトラフィック フローを関連する Guard の保護モジュールに誘導します。
- バイパス フィルタ：特定のトラフィック フローが Guard の保護メカニズムによって処理されないように防止します。
- フレックスコンテンツ フィルタ：指定されたパケット フローをカウントまたはドロップします。フレックスコンテンツ フィルタは、バークリー パケット フィルタとパターン フィルタを組み合せたもので、IP ヘッダーと TCP ヘッダーのフィールドに基づいたフィルタリングやコンテンツのバイト数に基づいたフィルタリングなど、非常に柔軟なフィルタリング機能をユーザに提供します。
- 動的フィルタ：指定されたトラフィック フローを関連する Guard の保護モジュールに誘導します。Guard は、トラフィック フローを分析した結果として動的フィルタを作成します。この一連のフィルタは、ゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整されます。動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。

保護モジュール

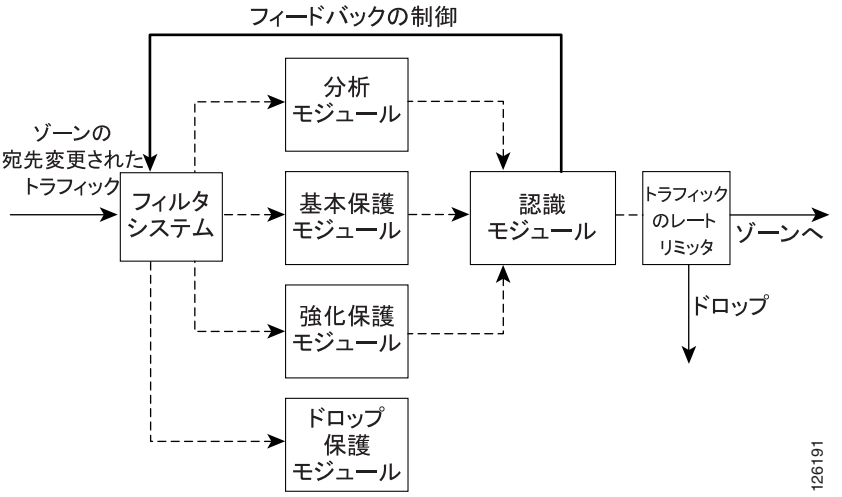
Guard モジュール の保護モジュールは、トラフィック フローにさまざまなプロセスを適用します。Guard には、次の保護モジュールがあります。

- 分析保護モジュール：この保護モジュールにより、トラフィックを監視状態で流すことができます。ただし、保護中も異常がトレースされていない間はトラフィックは影響を受けません。異常がトレースされると、トラフィック フローは適切な保護モジュールに誘導されます。
- 基本保護モジュール：この保護モジュールは、トラフィックを認証するスプーフィング防止メカニズムとゾンビ防止メカニズムを提供します。これらのメカニズムは、疑わしいトラフィック フローを検査し、その送信元を確認します。
- 強化保護モジュール：この保護モジュールは、より強力なスプーフィング防止メカニズムを備えています。これらの認証メカニズムは、フローのパケット検査し、フローの正当性を確認します。
- ドロップ保護モジュール：この保護モジュールは、悪意のあるトラフィックをドロップします。
- レート リミット保護モジュール：この保護モジュールは、目的のトラフィック フローまたはゾーン トラフック全体のレートを制限します。
- 認識および統計保護モジュール：この保護モジュールは、ポリシーとフィルタ システム間の調整を行います。ゾーンのポリシーを適用し、ゾーンのトラフィックの異常を監視します。

保護サイクル

図 1-2 に、Guard の保護サイクルを示します。

図 1-2　Guard の保護サイクル



ゾーン保護がアクティブになると、Guard のポリシーはゾーンのトラフィック フローを監視します。ポリシーは、特定のトラフィック フローがポリシーのしきい値を超過すると、そのフローに対してアクションを実行します。ポリシーが実行するアクションは、単なる通知の発行から、新しいフィルタ（動的フィルタ）の作成にまで及びます。このフィルタは、宛先変更されたトラフィックを関連する保護モジュールに誘導します。保護モジュールは、このトラフィックを認証します。サンプルでは、トラフィックは認識保護モジュールに流れています。このモジュールでは、ゾーンのポリシーを適用し、ゾーンのトラフィックの異常を監視します。

Guard は、ゾーンに流れるトラフィックのレートを監視します。定義済みのレートを超過するトラフィックはドロップされ、正当なトラフィックはゾーンに転送されます。Guard は、ゾーンのトラフィックの統計分析を行い、クローズドループのフィードバック サイクルを制御して、動的に変化するゾーンのトラフィック特性や変化する DDoS 攻撃のタイプに合せて保護措置を調整します。

Guard は、使用されている動的フィルタがなくなり、ゾーンへのトラフィックがドロップされず、事前に定義された期間で新しい動的フィルタが追加されなかった場合に、ゾーン保護を停止します。

CHAPTER 2

スーパーバイザ エンジンへの Guard モジュールの設定

この章では、スーパーバイザ エンジンへの Cisco Anomaly Guard Module（Guard モジュール）の設定方法について説明します。

Cisco Anomaly Guard Module（Guard モジュール）は Cisco IOS アプリケーション モジュールの 1 つで、次の製品のどちらかに設置できます。

- Supervisor Engine 720（SUP720）、または Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を備えた Supervisor Engine 2（SUP2）が搭載された、Cisco Catalyst 6500 シリーズ スイッチ。Catalyst 6500 で Guard モジュールをサポートするには、IOS 12.2(18)SXD3 以降が必要です。
- SUP720 が搭載された Cisco 7600 シリーズ ルータ。7600 シリーズ ルータで Guard モジュールをサポートするには、IOS 12.2(18)SXE 以降が必要です。

この章は、次の項で構成されています。

- Guard モジュールの設置の確認
- Guard モジュールの管理の設定
- VLAN の設定
- Guard モジュールへの VLAN の割り当て
- VLAN へのレイヤ 3 インターフェイスの設定
- Guard モジュールとのセッションの確立
- Guard モジュールのリブート

- Guard モジュールの設定の確認
- 1 つのスイッチに対する複数の Guard モジュールの設定

スーパーバイザに Guard モジュールを設定するには、EXEC 特権を保有し、設定モードに入る必要があります。

フラッシュ メモリへの設定変更をすべて保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

Guard モジュールの設置の確認

スーパーバイザ エンジンで新しい Guard モジュールが認識され、オンラインになっていることを確認します。

（注） Catalyst 6500 シャーシ内に Guard モジュールを設置する方法については、『*Cisco Anomaly Guard Module and Traffic Anomaly Detector Module Installation Note*』を参照してください。

設置を確認するには、次の手順を実行します。

ステップ 1　スーパーバイザ エンジン コンソールにログインします。

ステップ 2　Guard モジュールがオンラインになっていることを確認します。次のコマンドを入力します。

```
show module
```

次の例は、**show module** コマンドの出力を示しています。

```
Sup# show module
Mod Ports Card                                  Type Model    Serial No.
--  ---   ---------------------                 ---------    ------
1   2     Catalyst 6000 supervisor 2(Active) WS-X6K-SUP2-2GESAL081230TJ
... ...
6   3     Anomaly Guard module Module           WS-SVC-AGM-1-K9SAD081000GG
Mod  MAC addresses                     Hw    Fw      Sw          Status
---  ------------------------------------ ------- ----------- -------
...
6    000e.847f.fe04 to 000e.847f.fe0b3.0   7.2(1)  4.0(0.10)   Ok
...
Sup#
```

（注）　Guard モジュールを初めて設置した場合、ステータスは通常 **other** になります。Guard モジュールが診断ルーチンを完了してオンラインになると、ステータスは **Ok** になります。Guard モジュールがオンラインになるまで、少なくとも 5 分かかります。

Guard モジュールの管理の設定

Guard モジュールとリモート管理セッションを確立するには、Guard モジュールの管理ポートを設定する必要があります。

管理のために VLAN を選択するには、次のコマンドを入力します。

anomaly-guard module *module_number* **port** *port_number* [**allowed-vlan** *vlan_range* | **native-vlan** *vlan_id*]

表 2-1 で、**anomaly-guard module** コマンドの引数とキーワードについて説明します。

表 2-1　anomaly-guard コマンドの引数

パラメータ	説明
module_number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
port_number	管理用に使用するポートの番号。Guard モジュールでは、管理用にポート *1* がサポートされています。
vlan_range	VLAN の範囲、またはカンマ区切りリストで指定するいくつかの VLAN（スペース文字を入力することはできません）。
vlan_id	802.1Q トランキング モードにおけるトランクのネイティブ VLAN を設定します。デフォルトのネイティブ VLAN は 1 です。

次の例は、シャーシの番号 *4* のスロットに装着されたモジュールについて、管理のために VLAN *5* を選択する方法を示しています。

```
Sup(config)# anomaly-guard module 4 port 1 allowed-vlan 5
```

Guard モジュールとリモート管理セッションを確立するには、次の事項も Guard モジュールに設定する必要があります。

- Guard モジュールの管理ポート インターフェイス eth1 を設定する。詳細については、P.3-9 の「物理インターフェイスの設定」を参照してください。
- 関連するサービスをイネーブルにする。詳細については、P.3-8 の「Guard モジュールのインターフェイスの設定」を参照してください。

VLAN の設定

トラフィックを Guard モジュールに転送するためのスーパーバイザ エンジンに VLAN を設定するには、次の手順を実行します。

ステップ 1　トラフィックを Guard モジュールに転送するためのスーパーバイザ エンジンに VLAN を設定します。詳細については、P.2-6 の「スーパーバイザ エンジンへの VLAN の設定」を参照してください。

ステップ 2　Guard モジュールに VLAN を割り当てます。詳細については、P.2-7 の「Guard モジュールへの VLAN の割り当て」を参照してください。

ステップ 3　（オプション）VLAN にレイヤ 3 インターフェイスを設定します。詳細については、P.2-8 の「VLAN へのレイヤ 3 インターフェイスの設定」を参照してください。

ステップ 4　Guard モジュールのインターフェイスを設定します。詳細については、P.3-8 の「Guard モジュールのインターフェイスの設定」を参照してください。

スーパーバイザ エンジンへの VLAN の設定

トラフィックを Guard モジュールに転送するには、スーパーバイザ エンジンに VLAN を設定する必要があります。スーパーバイザ エンジン上に VLAN を作成するには、**vlan** コマンドを入力し、Guard モジュールに割り当てる VLAN 範囲を定義します。次のコマンドを入力します。

vlan *vlan_range*

vlan_range 引数には、単一の番号、VLAN の範囲、またはカンマ区切りリスト形式の複数の VLAN を指定します（スペース文字を入力することはできません）。vlan_range は、1 つまたは複数の VLAN（1 ～ 4,094）となります。

例

```
Sup(config)# vlan 86-89,99
```

Guard モジュールへの VLAN の設定方法については、P.3-11 の「VLAN の設定」を参照してください。

Guard モジュールへの VLAN の割り当て

Guard モジュールに VLAN を割り当てるには、Guard モジュールとイーサネット ポート間のマッピングについて理解する必要があります。このイーサネット ポートとは、Guard モジュールをスイッチ ファブリックに接続するものを指します。

Guard モジュールに VLAN を割り当てるには、スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

anomaly-guard module *module_number* **port** *port_number* [**allowed-vlan** *vlan_range* | **native-vlan** *vlan_id*]

表 2-2 に、**anomaly-guard module** コマンドの引数を示します。

表 2-2　anomaly-guard module コマンドの引数

パラメータ	説明
module_number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
port_number	ポート番号（1 ～ 3）。ポート 1 は管理用に、ポート 2 はデータ用に使用されます。ポート 3 は現在使用されていません。
vlan_range	VLAN の範囲、またはカンマ区切りリストで指定するいくつかの VLAN（スペース文字を入力することはできません）。
vlan_id	802.1Q トランキング モードにおけるトランクのネイティブ VLAN を設定します。デフォルトのネイティブ VLAN は 1 です。 使用可能な VLAN の 1 つは、管理 VLAN である必要があります。デフォルトでは、VLAN *1* になっています。

例

```
Sup# anomaly-guard module 7 port 2 allowed-vlan 1,3,6-15
```

（注） Guard モジュールには、管理ポートとデータ ポートも設定する必要があります。詳細については、P.3-9 の「物理インターフェイスの設定」を参照してください。

VLAN へのレイヤ 3 インターフェイスの設定

アプリケーションで必要な場合は、VLAN にレイヤ 3 インターフェイスを設定できます。

（注） レイヤ 3 インターフェイスを設定する前に、Guard モジュールに VLAN を割り当てる必要があります。

レイヤ 3 VLAN インターフェイスを設定するには、次の手順を実行します。

ステップ 1　VLAN インターフェイス設定モードに入ります。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

interface vlan *vlan-id*

vlan-id 引数には、VLAN の番号を指定します。有効な値は 1 ～ 4,094 です。

ステップ 2　VLAN の IP アドレスを設定します。次のコマンドを入力します。

ip address *ip_address subnet_mask*

ip-addr 引数および *subnet-mask* 引数には、インターフェイスの IP アドレスを指定します。

ステップ 3　インターフェイスをアクティブにします。次のコマンドを入力します。

no shutdown

例

```
sup (config)# interface vlan 5
sup (config-if)# ip address 192.168.89.100 255.255.255.0
sup (config-if)# no shutdown
```

Guard モジュールとのセッションの確立

Guard モジュールにログインするには、次の手順を実行します。

ステップ 1　Telnet またはコンソールでスイッチにログインします。

ステップ 2　スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

```
session slot slot_number processor processor_number
```

表 2-3 に、**session slot** コマンドの引数を示します。

表 2-3　session slot コマンドの引数

パラメータ	説明
slot-number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
processor_number	Guard モジュールのプロセッサの番号。Guard モジュールは、プロセッサ *1* を使用した管理だけをサポートします。

Guard モジュール ログイン プロンプトで、次のコマンドを入力してログインします。

```
login: admin
```

ステップ 3　パスワードを入力します。

Guard モジュールとセッションを初めて確立する場合は、admin ユーザ アカウントと riverhead ユーザ アカウントのパスワードを選択する必要があります。パスワードは、スペースを含まず、6 ～ 24 文字の長さである必要があります。パスワードは、いつでも変更できます。詳細については、P.4-10 の「パスワードの変更」を参照してください。

ログインに成功すると、コマンドライン プロンプトの表示が **user@GUARD#** になります。このマニュアルでは、表記法としてこのプロンプトを使用します。**hostname** コマンドを入力することにより、このプロンプトを変更できます。

Guard モジュールのリブート

Cisco IOS には、Guard モジュールを制御するコマンドとして、**boot**、**shutdown**、**power enable**、および **reset** が用意されています。

注意　スーパーバイザ エンジン レベルで reload コマンドを発行すると、シャーシ全体でリロードが発生し、そのシャーシ内のすべてのモジュールが影響を受けます。Guard モジュールをリロードする方法については、P.12-7 の「Guard モジュールのリロード」を参照してください。

- **shutdown**：すべてのデータを確保して、オペレーティング システムを正しくシャットダウンします。Guard モジュールの破損を避けるには、Guard モジュールを正しくシャットダウンする必要があります。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  hw-module module *slot_number* **shutdown**

  slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。

  次に、Guard モジュールを再起動するには、**hw-module module** *module_number* **reset** コマンドを入力する必要があります。

  例

  ```
  Sup# hw-module module 8 shutdown
  ```

（注）　スイッチがリブートされると、Guard モジュールもリブートします。

- **reset**：モジュールをリセットします。このコマンドは通常、アップグレード プロセスで、AP イメージと MP イメージとの切り替え、またはシャットダウンからの復旧のために使用します。**hw-module reset** コマンドは、モジュールの電源をいったん切った後で入れ、モジュールをリセットします。リセット プロセスには数分かかります。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  hw-module module *slot_number* `reset [string]`

slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。*string* 引数は、PC ブート シーケンス用のオプションの文字列です。MP にリセットするには *cf:1* を、AP にリセットするには *cf:4* を入力します。詳細については、P.12-8 の「Guard モジュールのバージョンのアップグレード」を参照してください。

例

```
Sup# hw-module module 8 reset
```

- **no power enable**：モジュールをシャットダウンして、シャーシから安全に除去できるようにします。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  no power enable module *slot_number*

  slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。

  モジュールをもう一度オンにするには、次のコマンドを入力します。

  power enable module *slot_number*

  例

  ```
  Sup (config)# no power enable module 8
  ```

- **boot**：次回の電源投入時に Guard モジュールをメンテナンス パーティション（MP）からブートさせます。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  boot device module *slot_number* cf:1

  slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。

  次回のブート サイクルで Guard モジュールをデフォルト パーティション（AP）からブートできるようにするには、次のコマンドを入力します。

  no boot device module *slot_number* cf:1

  例

  ```
  Sup# boot device module 8 cf:1
  ```

注意　ゾーンのラーニング プロセスは、リブート後に再起動されます。リブート後のゾーンのデフォルト動作に関する詳細については、P.12-7 の「Guard モジュールのリブート」を参照してください。

Guard モジュールの設定の確認

スーパーバイザ エンジンに対する Guard モジュールの設定を確認するには、スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

show anomaly-guard module ***slot_number*** **port** *port_number* [**state** | **traffic**]

表 2-4 で、**show module** コマンドの引数とキーワードについて説明します。

表 2-4　show module コマンドの引数

パラメータ	説明
slot-number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
port_number	ポート番号（1 ～ 3）。ポート 1 は管理用に、ポート 2 はデータ用に使用されます。
state	指定のポートの設定を表示します。
traffic	指定のポートのトラフィック統計情報を表示します。

例

```
Sup# show anomaly-guard module 8 port 2 state
```

1 つのスイッチに対する複数の Guard モジュールの設定

スーパーバイザ エンジンが少なくとも 1 つ設置されていれば、1 つの Catalyst 6500 シリーズ スイッチに複数の Guard モジュールを設置できます。モジュールの正確な数については、該当するバージョンのリリース ノートを参照してください。

次の設定のどちらかに複数の Guard モジュールを設定できます。

- ロード シェアリング
- 冗長性と高いアベイラビリティ

ロード シェアリング

ゾーン トラフィックを処理するための複数の Guard モジュールを設定できます。スーパーバイザ エンジンは、ゾーン トラフィックを Guard モジュール間に均等に分散させます。同じ宛先に対する複数のルートのコストが等しい場合、スーパーバイザ エンジンは必ずトラフィックを Guard モジュール間に均等に分散させます。

ロード シェアリング用に複数の Guard モジュールを設定するには、次の操作を行います。

- すべての Guard モジュールにゾーンを定義する。詳細については、P.6-9 の「ゾーンのアトリビュートの設定」を参照してください。
- すべての Guard モジュールに、同じ宛先変更ハイジャックの重みを割り当てる。詳細については、P.5-11 の「ハイジャック」を参照してください。
- すべての Guard モジュールで、ゾーンに対する Guard モジュールのラーニング プロセスを同時にアクティブにする。詳細については、P.6-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。
- すべての Guard モジュールでゾーンの保護をアクティブにする。詳細については、P.6-35 の「ゾーンの保護」を参照してください。

（注） 半分以上の Guard モジュールにおいて機能が停止した場合、残りの Guard モジュールは、正当なトラフィックをゾーンに対する攻撃と見なす場合があります。

冗長性と高いアベイラビリティ

高いアベイラビリティを実現するために、2 つの Guard モジュール（または Guard モジュールのグループ）を設定できます。このようにすると、アクティブな Guard モジュールが使用不能になった場合に、スーパーバイザ エンジンがゾーン トラフィックをスタンバイ状態の Guard モジュールに宛先変更します。

スーパーバイザ エンジンは、より低コストのルート（重みが最小のルート）にトラフィックを転送します。アクティブな Guard へのルートがダウンしていることを検出した場合は、単に、冗長ルートにトラフィックを転送します。

Guard モジュールの冗長性を設定するには、次の操作を行います。

- 両方の Guard モジュールに同じゾーンを定義する。詳細については、P.6-9 の「ゾーンのアトリビュートの設定」を参照してください。
- アクティブな Guard モジュールに、より小さい宛先変更ハイジャックの重みを割り当てる。詳細については、P.5-11 の「ハイジャック」を参照してください。
- 冗長 Guard モジュールに、より大きい宛先変更ハイジャックの重みを割り当てる。詳細については、P.5-11 の「ハイジャック」を参照してください。
- アクティブな Guard で Guard モジュールのラーニング プロセスをアクティブにする。詳細については、P.6-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。
- ゾーン設定を冗長 Guard にコピーする。詳細については、P.12-2 の「設定のエクスポート」および P.12-4 の「設定のインポートとアップデート」を参照してください。
- 両方の Guard モジュールでゾーンの保護をアクティブにする。詳細については、P.6-35 の「ゾーンの保護」を参照してください。

CHAPTER 3

Guard モジュールの初期化

この章では、Cisco Anomaly Guard Module（Guard モジュール）をネットワークに接続し、管理するための基本的なタスクについて説明します。

この章は、次の項で構成されています。

- コマンドライン インターフェイスの使用
- Guard モジュールのインターフェイスの設定
- Guard モジュールのインターフェイスの設定
- デフォルト ゲートウェイの設定
- ルーティング テーブルへのスタティック ルートの追加
- プロキシ IP アドレスの設定
- Guard モジュールの管理

コマンドライン インターフェイスの使用

CLI を使用して、Guard モジュールの機能を制御できます。Guard モジュールのユーザ インターフェイスは、多数の異なるコマンド モードに分割されています。任意の時点で使用できるコマンドは、そのときのモードによって異なります。システム プロンプトで **?** と入力すると、各コマンド モードで使用可能なコマンドのリストを取得できます。

CLI へのアクセス権は、ユーザの特権レベルに対応しています。各特権レベルには、独自のコマンドのグループがあります。

表 3-1 に、ユーザの特権レベルの説明を示します。

表 3-1　ユーザの特権レベル

ユーザの特権レベル	説明
管理者（admin）	すべての操作にアクセスできます。
設定（config）	ユーザの定義、削除、および修正に関連する操作を除いて、すべての操作にアクセスできます。
ダイナミック（dynamic）	監視と診断、保護、およびラーニングに関する操作にアクセスできます。dynamic 特権を持つユーザは、フレックスコンテンツ フィルタおよび動的フィルタを設定することもできます。
表示（show）	監視操作と診断操作にアクセスできます。

（注） フィルタの設定はすべて、管理者の特権レベルまたは設定の特権レベルを持つユーザが実行することをお勧めします。これより下位の特権レベルしか持たないユーザも、動的フィルタを追加および削除できます。

この項では、次のトピックについて取り上げます。

- CLI でのコマンドの発行
- CLI 使用のヒント

CLI でのコマンドの発行

この項では、CLI コマンドの入力規則について説明した後、次のトピックについて取り上げます。

- コマンドの no 形の使用
- show コマンドの構文
- CLI のエラー メッセージ

表 3-2 に、CLI コマンドの入力規則をまとめます。

表 3-2　CLI の規則

目的の操作	キーボード シーケンス
コマンド履歴をスクロールして変更する	矢印キーを使用する
特定のコマンド モードで使用可能なコマンドを表示する	**Shift+?**
コマンドの補完を表示する	コマンドの最初の部分を入力し、**Tab** キーを押す
コマンド構文の補完を表示する	コマンドを入力して、**Tab** キーを 2 回押す
`more` コマンドを使用してスクロールする	**more** *number-of-lines* **more** コマンドでは、Space キーを押したときにウィンドウに表示される追加の行数が設定されます。デフォルトは、その端末で表示可能な行数より 2 行少ない行数です。 *number-of-lines* 引数は、Space キーを押したときに表示される追加の行数を設定します。
一画面分スクロールする（コマンド出力内）	**Space** キー
一画面分後方にスクロールする（コマンド出力内）	b キー
スクロール動作を中止する	q キー
文字列を前方に検索する	/ 文字列

表 3-2　CLI の規則（続き）

目的の操作	キーボード シーケンス
文字列を後方に検索する	? 文字列
アクションをキャンセルするか、パラメータを削除する	そのコマンドの **no** 形を使用する
現在の操作に関連する情報を表示する	show
現在のコマンド グループ レベルを終了して上位のグループ レベルに移る	exit
すべてのコマンド グループ レベルを終了してルート レベルに戻る	end
特定の *文字列* を含む最初の行も含めて、その行からコマンド出力を表示する	| begin *文字列*
特定の *文字列* を含むコマンド出力の行を表示する	| include *文字列*
特定の *文字列* を含まないコマンド出力の行を表示する	| exclude *文字列*

（注） ルート レベルで **exit** コマンドを使用すると、CLI 環境が終了し、オペレーティング システムのログイン画面に戻ります。

コマンドの no 形の使用

ほとんどすべての設定コマンドには、no 形も存在します。一般に、コマンドの no 形は、特定のフィーチャや機能をデイセーブルにする場合に使用します。ディセーブルになっているフィーチャや機能をイネーブルにするには、キーワード no のない状態でそのコマンドを使用します。たとえば、**event monitor** コマンドではイベント モニタが有効になり、**no event monitor** コマンドでは無効になります。

show コマンドの構文

ゾーン設定モードから、ゾーン関連の **show** コマンドを実行できます。また、これらのコマンドは、グローバル モードまたは設定モードからも実行できます。

グローバル モードまたは設定モードの **show** コマンドの構文は、次のとおりです。

show zone *zone-name parameters...*

ゾーン設定モードの **show** コマンドの構文は、次のとおりです。

show *parameters...*

（注） このマニュアルでは、明示的な指定がない限り、表記法として**ゾーン**設定モードの **show** コマンド構文を使用します。

CLI のエラー メッセージ

Guard モジュール CLI では、次の場合にエラー メッセージが表示されます。

- コマンドの構文が不完全であるか、間違っている場合。
- コマンドがシステムの設定と一致しない場合。
- システムの障害のために操作を実行できなかった場合。この場合は、システムのログにエントリが作成されます。

CLI 使用のヒント

この項では、CLI を使用する際のヒントになる、次のトピックについて取り上げます。

- ヘルプ
- タブ補完
- 操作の方向の規定
- コマンドの省略
- ワイルドカード文字

ヘルプ

CLI では、コマンド階層のすべてのモードで状況依存のヘルプが用意されています。ヘルプの情報では、現在のコマンド モードで使用可能なコマンドが示され、各コマンドの簡単な説明が提供されます。

ヘルプを取得するには、**?** と入力します。

コマンドのヘルプを表示するには、そのコマンドの後ろに **?** を入力します。

コマンド プロンプトで ? と入力すると、そのモードで使用可能なすべてのコマンドと、その短い説明が表示されます。

ヘルプには、現在のモードで使用可能なコマンドのみが表示されます。

タブ補完

コマンドの一部を入力して Tab キーを押すことにより、コマンドを補完することができます。

複数のオプションを取る値を持ったコマンドを入力し、Tab キーを 2 回押すと、使用可能な入力パラメータが表示されます。この機能は、システム定義パラメータにもユーザ定義パラメータにも使用できます。
たとえば、ゾーン設定モードで **policy-template** コマンドを入力し、Tab キーを 2 回押すと、ポリシー テンプレート名のリストが表示されます。設定モードで **zone** コマンドを入力し、Tab キーを 2 回押すと、定義済みのゾーンが表示されます。

タブ補完で複数のコマンドが一致する場合は、何も表示されず、端末には入力されている現在の行がもう一度表示されます。

タブ補完とヘルプでは、現在のモードで使用可能なコマンドのみが表示されます。

操作の方向の規定

一般に、コマンド名の前に ftp がある場合は、コマンドの方向は Guard モジュールから FTP サーバへのコピーになります。コマンドが ftp の前にある場合には、コマンドの方向は FTP サーバから Guard モジュールへのコピーになります。たとえば、**copy log ftp** コマンドではログ ファイルが FTP サーバにコピーされます。**copy ftp new-version** コマンドでは、新規バージョンが FTP サーバから Guard モジュールにコピーされます。

コマンドの省略

コマンドやキーワードは、一意な省略形を保てる文字数まで短縮できます。

たとえば、**show** コマンドは **sh** まで短縮できます。

ワイルドカード文字

ワイルドカードとして、アスタリスク（*）を使用できます。

例

learning policy-construction * コマンドを発行すると、Guard モジュールに設定されたすべてのゾーンでポリシー構築フェーズがアクティブになります。

learning policy-construction scan* コマンドを発行すると、scan で始まる名前を持つ、Guard モジュールに設定されたすべてのゾーン（scannet や scanserver など）でポリシー作成フェーズがアクティブになります。

no zone * コマンドを発行すると、すべてのゾーンが削除されます。

Guard モジュールのインターフェイスの設定

この項では、Guard モジュールのインターフェイスの設定手順を説明します。Guard モジュールは、スーパーバイザ上に 1 つの管理ポートと 2 つのデータ ポートを備えています。

現在のバージョンでは、データ ポートは 1 つだけが使用されています。

Guard モジュールを設定するには、設定モードに入る必要があります。

次のコマンドを入力します。

configure [**terminal**]

例

```
user@GUARD# configure
user@GUARD-conf#
```

Guard モジュールを正しく機能させるためには、Guard モジュールのインターフェイスを設定する必要があります。インターフェイスの特性には、IP アドレスやインターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）などがあります。

注意　同じサブネット上に 2 つの物理インターフェイスを設定しないでください。

多くの機能は、インターフェイス単位でイネーブルになります。**interface** コマンドを入力するときには、インターフェイスのタイプと番号を指定する必要があります。

次の一般的なガイドラインは、すべての物理および仮想インターフェイスの設定プロセスに当てはまります。

- 各インターフェイスには、IP アドレスと IP サブネット マスクを設定する必要があります。
- **no shutdown** コマンドを使用して、各インターフェイスをアクティブにする必要があります。

インターフェイスの設定を表示するには、**show** コマンドまたは
show running-config コマンドを使用します。

物理インターフェイスの設定

物理インターフェイスを設定するには、次の手順を実行します。

ステップ 1　インターフェイス設定モードに入ります。設定モードで次のコマンドを入力します。

```
interface if-name
```

if-name 引数には、インターフェイス名を指定します。

Guard モジュールは、次のインターフェイスをサポートします。

- eth1：管理ポート
- giga2：データ ポート

ステップ 2　インターフェイスの IP アドレスを設定します。次のコマンドを入力します。

```
ip address ip-addr ip-mask
```

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します（たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0）。

ステップ 3　（オプション）インターフェイスの MTU を定義します。次のコマンドを入力します。

```
mtu integer
```

integer 引数は、eth1 インターフェイスの場合は 576 ～ 16,384 バイトの整数で、giga2 インターフェイスの場合は 576 ～ 1,824 の整数です。

デフォルトの MTU の値は 1,500 バイトです。

ステップ 4　（オプション）インターフェイスの速度とデュプレックス モードを設定します。次のコマンドを入力します。

speed {auto | half *speed* | full *speed*}

表 3-3 で、**speed** コマンドの引数とキーワードについて説明します。

表 3-3　speed コマンドの引数とキーワード

パラメータ	説明
auto	インターフェイスのオートネゴシエーション機能を有効にします。インターフェイスは、ネットワーク設定で使用されているメディア タイプ、およびピア ルータ、ハブ、スイッチの伝送速度などの環境要因に応じて、10 Mbps、100 Mbps、1000 Mbps のいずれか、半二重または全二重で自動的に動作します。 これがデフォルトのモードです。
half	半二重動作を指定します。
full	全二重動作を指定します。
speed	インターフェイスの速度。10、100、または 1000 を、それぞれ 10Mbps、100Mbps、および 1000Mbps として入力します。

ステップ 5　インターフェイスをアクティブにします。次のコマンドを入力します。

no shutdown

設定の変更を有効にするには、Guard モジュールをリロードする必要があります。

例

```
user@GUARD-conf# interface eth1
user@GUARD-conf-if-eth1# ip address 10.10.10.33 255.255.255.252
user@GUARD-conf-if-eth1# no shutdown
```

物理インターフェイスを非アクティブにするには、**shutdown** コマンドを使用します。

VLAN の設定

データ ポートに VLAN を定義できます。

VLAN を定義するには、次の手順を実行します。

ステップ 1　VLAN　インターフェイスが存在する場合は、その設定モードに入ります。または、新しい VLAN を定義します。設定モードで次のコマンドを入力します。

interface giga2.*vlan-id*

vlan-id 引数は、VLAN ID 番号を指定する整数です。VLAN ID は、TAG IEEE 802.1Q に従った番号です。

ステップ 2　VLAN の IP アドレスを設定します。次のコマンドを入力します。

ip address *ip-addr ip-mask*

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します（たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0）。

ステップ 3　（オプション）インターフェイスの MTU を定義します。次のコマンドを入力します。

mtu *integer*

integer 引数は、576 ～ 1,824 バイトの整数です。

デフォルトの MTU の値は 1,500 バイトです。

ステップ 4　インターフェイスをアクティブにします。次のコマンドを入力します。

```
no shutdown
```

例

```
user@GUARD-conf#interface giga2.2
user@GUARD-conf-if-giga2.2# ip address 192.168.5.8 255.255.255.0
user@GUARD-conf-if-giga2.2# no shutdown
```

ループバック インターフェイスの設定

ループバック インターフェイスを設定できます。

ループバック インターフェイスを設定するには、次の手順を実行します。

ステップ 1　ループバック インターフェイスが存在する場合は、その設定モードに入ります。または、新しいループバック インターフェイスを定義します。設定モードで次のコマンドを入力します。

```
interface if-name
```

if-name 引数には、ループバック インターフェイス名を指定します。インターフェイス名は、**lo:***integer* で、*integer* は 0 ～ 1,023 の整数です。

ステップ 2　ループバック インターフェイスの IP アドレスを設定します。次のコマンドを入力します。

```
ip address ip-addr ip-mask
```

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します（たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0）。

ステップ 3　ループバック インターフェイスの設定モードを終了します。次のコマンドを入力します。

```
exit
```

例

```
user@GUARD-conf# interface lo:0
user@GUARD-conf-if-lo:0# ip address 1.1.1.1 255.255.255.255
user@GUARD-conf-if-lo:0# exit
```

デフォルト ゲートウェイの設定

Guard モジュールにデフォルト ゲートウェイを割り当てることができます。ほとんどの場合、Guard モジュールのデフォルト ゲートウェイの IP アドレスは、Guard モジュールとインターネットの間に存在する隣接ルータです。デフォルト ゲートウェイ アドレスは、Guard モジュールのネットワーク インターフェイスの IP アドレスのいずれかと同じネットワーク上にある必要があります。

（注） Guard モジュールが保護モードのときには、デフォルト ゲートウェイに IP アドレスを割り当てないでください。

注意 デフォルト ゲートウェイ アドレスを削除すると、Guard モジュールにアクセスできなくなる場合があります。

デフォルト ゲートウェイ アドレスを割り当てるには、次のコマンドを入力します。

default-gateway *ip-addr*

ip-addr 引数には、デフォルト ゲートウェイの IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。

デフォルト ゲートウェイ アドレスを変更するには、このコマンドを再発行します。

例

```
user@GUARD-conf# default-gateway 192.168.100.1
```

ルーティング テーブルへのスタティック ルートの追加

Guard モジュールのルーティング テーブルにスタティック ルートを追加できます。スタティック ルートは、Guard モジュールの IP インターフェイスに関連付けられたローカル ネットワークの外側にあるサーバやネットワークのルートを指定するために追加します。

スタティック ルートは永続的に追加され、Guard モジュールのリブート後も削除されません。

Guard モジュールのルーティング テーブルにスタティック ルートを追加するには、次のコマンドを入力します。

ip route *ip-addr ip-mask nexthop-ip* [*if-name*]

表 3-4 に、**ip route** コマンドの引数を示します。

表 3-4　ip route コマンドの引数

パラメータ	説明
ip-addr	ルートの宛先ネットワーク。宛先には、IP ネットワーク アドレス（ネットワーク アドレスのホスト ビットは 0 に設定）またはホスト ルートの IP アドレスを指定できます。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
ip-mask	宛先ネットワークに関連付けられたサブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。
nexthop-ip	宛先ネットワークとサブネット マスクによって定義された一連のアドレスへの到達を可能にする転送アドレスまたはネクスト ホップ IP アドレス。ネクスト ホップ IP アドレスは、インターフェイスのサブネット内にある必要があります。ローカル サブネット ルートでは、ネクスト ホップ IP アドレスは、そのサブネットに接続されたインターフェイスに割り当てられている IP アドレスです。1 つ以上のルータをまたいで使用可能なリモート ルートの場合、ネクスト ホップ IP アドレスは、ネイバー ルータに割り当てられている直接到達可能な IP アドレスです。

表 3-4　ip route コマンドの引数（続き）

パラメータ	説明
if-name	（オプション）宛先への到達が可能な Guard モジュールのインターフェイスまたは VLAN。インターフェイスを指定しない場合、使用されるインターフェイスは、Guard モジュールのルーティング テーブルに従ってネクスト ホップ IP アドレスから判別されます。

例

```
user@GUARD-conf# ip route 172.16.31.5 255.255.255.255 192.168.100.34
```

ルーティング テーブルを表示するには、**show ip route** コマンドを使用します。

プロキシ IP アドレスの設定

Guard モジュールには、プロキシ IP アドレスを割り当てる必要があります。Guard モジュールのプロキシ IP アドレスは、プロキシ モードのスプーフィング防止保護メカニズムで必要です。Guard モジュールが保護モードのときには、Guard モジュールにプロキシ IP アドレスを割り当てないでください。

警告　**ゾーン保護モードをアクティブにするには、プロキシ IP アドレスを定義する必要があります。**

Guard モジュールのスプーフィング防止用プロキシ IP アドレスを設定するには、次のコマンドを入力します。

proxy *ip-addr*

ip-addr 引数には、プロキシ IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。

各ゾーンと Guard モジュールのプロキシ IP アドレス間のルートを確認する必要があります。Guard モジュールは、プロキシ IP アドレスに対する ping 要求には応答しません。

追加のプロキシ IP アドレスを設定するには、このコマンドを再発行します。

ネットワークでロード バランシングを使用してネットワークの過負荷を分散している場合、または多数の同時接続が必要な場合は、プロキシ IP アドレスを 3 つまたは 4 つ設定することをお勧めします。

Guard モジュールでは、プロキシ IP アドレスを最大 10 個使用できます。

Guard モジュールの管理

スーパーバイザからセッションを確立し、Guard モジュールのネットワーク機能を設定した後は（第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」と P.3-8 の「Guard モジュールのインターフェイスの設定」を参照）、次のいずれかの方法を使用して Guard モジュールにアクセスし、管理することができます。

- セキュリティ保護されたシェル（SSH）のセッションを使用したアクセス。詳細については、P.3-19 の「SSH を使用した Guard モジュールへのアクセス」を参照してください。
- Web ベース管理（WBM）を使用した Guard モジュールへのアクセス。詳細については、P.3-18 の「Web ベース管理による Guard モジュールの管理」を参照してください。
- DDoS 検知からのアクセス。DDoS 検知は、接続を確立し、DDoS 対抗システムを形成するネットワーク要素です。詳細については、該当するマニュアルを参照してください。

Web ベース管理による Guard モジュールの管理

Web ベース管理（WBM）を使用すると、Web ブラウザを使用して Web から Guard モジュールを管理できます。

Guard モジュールの WBM をイネーブルにするには、次の手順を実行します。

ステップ 1　WBM サービスをイネーブルにします。次のコマンドを入力します。

```
service wbm
```

ステップ 2　リモート マネージャの IP アドレスから Guard モジュールへのアクセスを許可します。次のコマンドを入力します。

```
permit wbm ip-addr [ip-mask]
```

ip-addr 引数および *ip-mask* 引数には、リモート マネージャの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します。

ステップ 3　ブラウザを開いて、次のアドレスを入力します。

https://*Guard Module-ip-address*/

Guard Module-ip-address 引数は、Guard モジュールの IP アドレスです。

Guard モジュールの WBM ウィンドウが表示されます。

（注）　Web ベース管理をイネーブルにするには、HTTP ではなく HTTPS が使用されます。

ステップ 4　ユーザ名とパスワードを入力して、**OK** をクリックします。

ユーザ名とパスワードを正しく入力すると、Guard のホームページが表示されます。

TACACS+ 認証が設定されている場合は、ユーザ認証にローカル データベースではなく TACACS+ ユーザ データベースが使用されます。

例

```
user@GUARD-conf# service wbm
user@GUARD-conf# permit wbm 192.168.30.32
```

SSH を使用した Guard モジュールへのアクセス

セキュリティ保護されたシェル（SSH）の接続を使用して、Guard モジュールにアクセスすることができます。この項では、Guard モジュールの SSH 通信設定について説明します。

SSH サービスは、デフォルトでイネーブルになっています。

Guard モジュールへの SSH 接続をイネーブルにするには、次の手順を実行します。

ステップ 1　リモート ネットワーク IP アドレスから Guard モジュールへのアクセスを許可します。次のコマンドを入力します。

```
permit ssh ip-addr [ip-mask]
```

ip-addr 引数および *ip-mask* 引数には、リモート ネットワークの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します。

ステップ 2　リモート ネットワーク アドレスから接続を確立し、ログイン名とパスワードを入力します。ログイン名とパスワードを入力せずに SSH 接続をイネーブルにするには、Guard モジュールの SSH 鍵リストにリモート接続の SSH 公開鍵を追加します。詳細については、P.4-31 の「SSH 鍵の管理」を参照してください。

CHAPTER 4

Guard モジュールの設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）のサービスの設定方法について説明します。

この章には、次の主要な項があります。

- Guard モジュールのサービスのアクティブ化
- アクセス コントロールの設定：認証、認可、アカウンティングの使用
- Cisco Traffic Anomaly Detector Module との通信のイネーブル化
- 日付と時刻の設定
- SSH 鍵の管理
- SFTP 接続の鍵の設定
- ホスト名の変更
- SNMP トラップのイネーブル化
- SNMP コミュニティ ストリングの設定

Guard モジュールのサービスのアクティブ化

Guard モジュールでアクティブにするサービスを定義することができます。正しい機能をイネーブルにするためには、サービスをイネーブルにして、そのサービスへのアクセスを許可する必要があります。Guard モジュールのサービスのアクティベーションを制御し、特定の IP アドレスに対してアクセス権を付与または拒否することにより、Guard モジュールにアクセスし、制御する IP アドレスを制限することができます。

表 4-1 で、Guard モジュールのサービスについて説明します。

表 4-1　Guard モジュール サービス

サービス	説明
internode-comm	ノード間通信サービス。Guard モジュールは、Cisco Traffic Anomaly Detector Module と通信チャネルを確立するときにこのサービスを使用します。
snmp-server	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）サーバ サービス。SNMP を使用して Guard モジュールにアクセスすることにより、Riverhead 管理情報ベース（Riverhead の専用 MIB、MIB2、および UCDavis の MIB）で定義された情報を取得することができます。 MIB 定義の詳細については、このバージョンに付属の MIB ファイルを参照してください。 **（注）** Riverhead MIB には、64 ビットのカウンタが含まれています。MIB を読み取るには、SNMP バージョン 2 をサポートするブラウザを使用する必要があります。
snmp-trap	SNMP トラップ サービス。snmp-trap サービスをアクティブにすると、Guard モジュールは SNMP トラップを生成します。詳細については、P.4-36 の「SNMP トラップのイネーブル化」を参照してください。

表 4-1　Guard モジュール サービス（続き）

サービス	説明
ssh	Secured Shell サービス（詳細については、P.4-31 の「SSH 鍵の管理」を参照）。
wbm	Web-Based Management（WBM）サービス。Web ブラウザを使用して、Web 経由で Guard モジュールを制御できます。

Guard モジュールのサービスをアクティブにするには、次の手順を実行します。

ステップ 1　Guard モジュールのサービスをイネーブルにします。次のコマンドを入力します。

```
service {internode-comm | snmp-server | snmp-trap | wbm}
```

Guard モジュールのサービスの説明については、表 4-1 を参照してください。デフォルトでは、SSH 以外、Guard モジュールのすべてのサービスはディセーブルになっています。

ステップ 2　Guard　モジュールのサービスに対するアクセス権を付与し、接続を可能にします。次のコマンドを入力します。

```
permit service ip-address-general [ip-mask]
```

表 4-2 に、**permit** コマンドの引数を示します。

表 4-2　permit コマンドの引数

パラメータ	説明
service	アクセスと操作の対象となるサービス。Guard モジュールのサービスの説明については、表 4-1 を参照してください。
ip-address-general	アクセスを許可する IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。すべての IP アドレスからのアクセスを許可するには、アスタリスク（*）を使用します。
ip-mask	（オプション）IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。

注意　セキュリティ上の理由から、すべての IP アドレスからのサービスへのアクセスを許可する（* と入力する）ことは推奨しません。

例

```
user@GUARD-conf# service wbm
user@GUARD-conf# permit wbm 192.168.10.35
```

アクセス コントロールの設定：認証、認可、アカウンティングの使用

アクセス コントロールとは、Guard モジュールにアクセスできるユーザ、およびアクセス権を持ったユーザが使用できるサービスを制御することです。認証、認可、アカウンティング（AAA）のセキュリティ サービスは、アクセスを設定するための基本的なフレームワークとなります。

- 認証：ユーザにシステムおよびシステム　サービスへのアクセスを許可する前に、そのユーザを識別する方法。
- 認可：システムへのアクセスを取得した後で、ユーザが実行することのできる内容を決定するプロセス。通常、このプロセスは、ユーザが認証され、システムの操作を開始した後で実行されます。
- アカウンティング：ユーザが実行中または実行済みの内容を記録する処理。アカウンティングにより、ユーザがアクセスしているサービスを追跡することができます。

Guard モジュールには、次のシステム ユーザ アカウントが事前設定されています。

- admin：admin ユーザ アカウントには、管理者アクセス権が設定されています。そのため、Guard モジュールの CLI とその機能にアクセスできます。Guard モジュールの CLI に初めて接続するときは、このアカウントのパスワードを設定する必要があります。新しいユーザ アカウントを設定するには admin ユーザ アカウントを使用します。
- riverhead：riverhead ユーザ アカウントには、ダイナミック（dynamic）のアクセス権が設定されています。Guard モジュールでは、このユーザ アカウントを使用して、Cisco Traffic Anomaly Detector Module と通信します。Guard モジュールの CLI に初めて接続するときは、このアカウントのパスワードを設定する必要があります。

  Cisco Traffic Anomaly Detector Module は、riverhead ユーザ名を使用して Guard をリモートでアクティブにできます。

システム ユーザ アカウントは削除できません。

ユーザ定義を使用すると、Guard モジュールのユーザ コミュニティをドメインに分割し、安全な管理アクセスのために必要に応じてパスワードを割り当てることができます。初期設定が完了した後は、ユーザのアクションを監視できるように新しいアカウントを作成し、システム ユーザ アカウントは使用しないことをお勧めします。

次の各項では、アクセス コントロールの設定方法について説明します。

- 認証の設定
- 認可の設定
- アカウンティングの設定
- TACACS+ サーバのアトリビュートの設定

認証の設定

ユーザが Guard モジュールにログインしようとするとき、または（**enable** コマンドを使用して）上位の特権レベルを要求するときに、Guard モジュールで使用する認証方式を設定することができます。Guard モジュールは、次の認証オプションを提供します。

- ローカル認証：ローカル認証では、ローカルに設定されたログイン名およびイネーブル パスワードが認証に使用されます。これはデフォルトの認証方式です。詳細については、P.4-8 の「ローカル認証の設定」を参照してください。
- TACACS+ 認証：TACACS+ 認証では、1 つの TACACS+ サーバまたは複数の TACACS+ サーバのリストを使用してユーザが認証されます。

  ユーザを 1 つの TACACS+ サーバにしか設定しない場合、その TACACS+ サーバで当該ユーザに対して認可も設定する必要があります。設定しないと、そのユーザは show コマンドにしかアクセスできません。

シーケンシャルな認証リストを設定することができます。認証リストでは、ユーザの認証に使用する認証方式を定義します。この定義により、認証に使用する 1 つ以上の方式を指定することができます。したがって、最初の方式が失敗した場合は、認証のバックアップ システムが提供されます。

Guard モジュールは、最初にリストされた方式を使用してユーザを認証します。その方式が応答しない場合、Guard モジュールは 2 番目の認証方式を選択します。両方の認証方式を試してもうまくいかない場合、認証は失敗します。

分散認証方式を設定することもできます。Guard モジュールは、最初の TACACS+ サーバを使用してユーザを認証します。認証で拒否が返された場合、Guard モジュールは TACACS+ サーバ リスト、および、存在する場合は代替の認証方式（ローカル）をスキャンします。リストをすべて試してもうまくいかない場合、認証は失敗します。このオプションは、*first-hit* オプションを設定していない場合にのみ有効です。

（注）　ユーザ データベースが、複数の TACACS+ サーバに分散している、または 1 つの TACACS+ サーバとローカル ユーザ データベースに分散している場合は、**no tacacs-server first-hit** コマンドを使用してください。

認証方式の設定

Guard モジュールで使用する認証方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認証が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.4-18 の「TACACS+ サーバのアトリビュートの設定」を参照してください。

ステップ 2　認証方式を定義します。次のコマンドを入力します。

```
aaa authentication {enable | login} {local | tacacs+}
[tacacs+ | local]
```

表 4-3 に、**aaa authentication** コマンドの引数を示します。

表 4-3　aaa authentication コマンドのキーワード

パラメータ	説明
enable	Guard モジュールは、上位の特権レベルに入るときに認証を行います。
login	Guard モジュールへのログイン時に認証が行われます。
local	Guard モジュールは、ローカル データベースを使用してユーザを認証します。
tacacs+	TACACS+ サーバによってユーザが認証されます。
tacacs+ | local	（オプション）設定された方式が失敗した場合の代替認証方式を設定します。

コンソール セッションから Guard モジュールにアクセスした場合、Guard モジュールは、定義済みの認証方式に関係なく、ローカル ユーザ データベースを使用して認証します。

認証方式を変更するには、このコマンドを再入力します。

次の例は、上位の特権レベルに入る際に認証を行うように設定する方法を示しています。最初の認証方式は TACACS+ に設定され、2 番目の認証方式はローカル ユーザ データベースに設定されています。

```
user@GUARD-conf# aaa authentication enable tacacs+ local
```

ローカル認証の設定

Guard モジュールには、管理者特権を持つユーザ名があらかじめ設定されています。このユーザ名を使用して新しいユーザを作成できます。ユーザ定義を使用すると、Guard モジュールのユーザ コミュニティをドメインに分割し、安全な管理アクセスのために必要に応じてパスワードを割り当てることができます。

1 つの TACACS+ サーバを使用した CLI ユーザの認証をイネーブルにするには、P.4-6 の「認証の設定」を参照してください。

ユーザの追加

Guard モジュールのローカル データベースにユーザを追加するには、次のコマンドを入力します。

username *username* {**admin** | **config** | **dynamic** | **show**} [*password*]

表 4-4 に、**username** コマンドの引数とキーワードを示します。

表 4-4　username コマンドの引数とキーワード

パラメータ	説明
username	ユーザ名。1 ～ 63 文字の英数字の文字列です。大文字と小文字が区別され、先頭は英字である必要があります。この文字列にはスペースを含めることはできませんが、アンダースコアを含めることはできます。
admin | **config** | **dynamic** | **show**	ユーザの特権レベル。詳細については、表 3-1 を参照してください。
password	（オプション）パスワード。6 ～ 24 文字の文字列を入力します。スペースは使用できず、大文字と小文字が区別されます。パスワードを入力しない場合、入力するよう要求されます。

例

```
user@GUARD-conf# username Robbin config 1234
```

ユーザはパスワードをクリア テキストで入力しますが、Guard モジュールの設定ファイルでは、パスワードは暗号化されて表示されます。次に、Guard モジュールの設定ファイル（running-config）の表示例を示します。

```
username Richard config encrypted 840xdMk3
```

上の例の encrypted オプションは、パスワードが暗号化されていることを示しています。

Guard モジュールに設定されたユーザのリストを表示するには、**show running-config** コマンドまたは **show guard** コマンドを使用します。現在 CLI にログインしているユーザのリストを表示するには、**show users** コマンドを使用します。

Guard モジュールのユーザ リストからユーザを削除するには、**no username** *username* コマンドを使用します。

パスワードの変更

ユーザは、自分自身のパスワードを変更することができます。管理者は、自分自身のパスワードと、他のすべてのユーザのパスワードを変更できます。

自分自身のパスワードを変更するには、次の手順を実行します。

ステップ 1　次のコマンドを入力します。

password

ステップ 2　現在のパスワードを入力します。新しいパスワードの入力を求めるプロンプトが表示されます。

ステップ 3　新しいパスワードを入力します。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

例

```
user@GUARD# password
Old Password: <old-password>
New Password: <new-password>
Retype New Password: <new-password>
```

管理者は、他のユーザのパスワードを変更できます。

特定のユーザのパスワードを変更するには、次の手順を実行します。

ステップ 1　グローバル モードで次のコマンドを入力します。

password *username-password*

username-password 引数は、変更対象のパスワードを持つユーザです。

ステップ 2　新しいパスワードを入力します。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

次の例では、管理者はユーザ *John* のパスワードを変更しています。

```
user@GUARD# password Jose
New Password: <new-password>
Retype New Password: <new-password>
```

認可の設定

ユーザが使用できるサービスを制限することができます。認可がイネーブルの場合、Guard モジュールはユーザのプロファイルでそのユーザのアクセス権を確認します。プロファイルは、ローカル ユーザ データベースまたは TACACS+ セキュリティ サーバにあります。ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。

ユーザがコマンドを実行しようとするときに Guard モジュールで使用する認可方式を設定することができます。Guard モジュールでは、次の認可オプションが提供されています。

- TACACS+ 認可：TACACS+ 認可では、TACACS+ サーバを使用してユーザが認可されます。後続のサーバが定義されている場合は、1 つのサーバとの通信が失敗した場合にのみ、そのサーバへのアクセスが開始されます。

  TACACS+ 認可では、2 種類がサポートされています。実行認可では、ユーザが Guard モジュールへのログイン時に認証されるときに、一度ユーザの特権レベルが決定されます。コマンド認可では、ユーザがコマンドを入力すると、各コマンドの認可を取得するために TACACS+ サーバに対して確認が行われます。

  TACACS+ 認可では、コマンドごとにアクセス権を指定することができます。

注意　**copy running-config** コマンドへの認可の付与には注意を払うことをお勧めします。
copy running-config コマンドの実行を認可すると、設定ファイル内ですべてのコマンドにそれぞれ認可を設定しているかどうかに関係なく、すべての設定コマンドに対して認可が与えられます。

- ローカル認可：ローカル認可では、コマンド グループのアクセス コントロールにローカルで設定されたユーザ プロファイルが使用されます。許可は、指定された特権レベルのすべてのコマンドに対して定義されます。これはデフォルトの認可方式です。

シーケンシャルな認可リストを設定することができます。認可リストでは、ユーザの認可に使用する認可方式を定義します。この定義により、認可に使用する 1 つ以上の方式を指定することができます。したがって、最初の方式に対する通信が失敗した場合は、認可のバックアップ システムが提供されます。

Guard モジュールは、最初にリストされた方式を使用してユーザを認可します。その方式が応答しない場合、Guard モジュールは 2 番目の認可方式を選択します。両方の認可方式が成功しなかった場合、認可は失敗します。

Guard モジュールのローカル認可は、TACACS+ サーバへの通信に失敗した場合に実行することができます。

ローカル許可の設定

Guard のサービスにアクセスできるかどうかは、ユーザの特権レベルによって決まります。システム管理者は、ユーザが使用できるサービスを制限することができます。Guard モジュールは、ユーザのプロファイルをチェックして、ユーザのアクセス権を確認します。認可されると、ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。ユーザの特権レベルについては、表 3-1 を参照してください。

パスワードを使用した特権レベルの割り当て

管理者は、ユーザの特権レベルへのアクセスを制限するパスワードを設定できます。

ローカル パスワードを設定して特権レベルへのアクセスを制御するには、次のコマンドを入力します。

enable password [**level** *level*] [*password*]

表 4-5 で、**enable password** コマンドの引数について説明します。

表 4-5　enable password コマンドの引数

パラメータ	説明
level	（オプション）目的の特権レベル。このレベルには、admin、config、dynamic、show のいずれかを指定できます。詳細については、表 3-1 を参照してください。デフォルトのレベルは admin です。
password	（オプション）特権レベルのパスワード。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。パスワードを入力しない場合、入力するよう要求されます。

例

```
user@GUARD-conf# enable password level admin <password>
```

ユーザ特権レベル間の移動

認可されたユーザは、ユーザ特権レベル間を移動することができます。

ユーザ特権レベル間を移動するには、次の手順を実行します。

ステップ 1　次のコマンドを入力します。

```
enable [level]
```

level 引数には、目的の特権レベルを指定します。このレベルには、admin、config、dynamic のいずれかを指定できます。デフォルトのレベルは **admin** です。詳細については、表 3-1 を参照してください。

ステップ 2　特権レベルのパスワードを入力します。

例

```
user@GUARD> enable admin
Enter enable admin Password: <password>
```

下位の特権レベル（show）に戻る場合は、disable コマンドを使用します。

認可方式の設定

認可方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認可が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.4-18 の「TACACS+ サーバのアトリビュートの設定」を参照してください。

ステップ 2　認可方式を定義します。次のいずれかのコマンドを入力します。

- **aaa authorization exec tacacs+**
- **aaa authorization commands** *level* {**local** | **tacacs+**} [**local**]

認可方式のシーケンシャルなリストを設定できます。各方式について、**aaa authorization** コマンドを入力します。認証方式を削除するには、このコマンドの no 形を使用します。

表 4-6 に、**aaa authorization** コマンドの引数とキーワードを示します。

表 4-6　aaa authorization コマンドの引数とキーワード

パラメータ	説明
exec	ユーザが EXEC シェルの実行を許可されているかどうかを判別するために認可が実行されます。Guard モジュールは、TACACS+ サーバに確認して、認証されたユーザの特権レベルを判別します。 **注意**　認可を設定する前に、TACACS+ サーバにそのユーザを設定しておく必要があります。これを行わないと、Guard モジュールにアクセスできない場合があります。
commands	指定された特権レベルのすべてのコマンドに対して認可が実行されます。複数の特権レベルの認可を設定するには、認可が必要な特権レベルごとにこのコマンドを発行します。
level	指定された特権レベルの認可を定義します。有効なエントリは、show、dynamic、config、および admin です。ユーザの特権レベルについては、表 3-1 を参照してください。
local	Guard モジュールのローカル データベースでユーザのアクセス権を確認します。
tacacs+	TACACS+ サーバでユーザのアクセス権を確認します。
local	（オプション）設定された認可方式が失敗した場合の代替の認可方式を設定します。

パフォーマンスへの影響を考慮し、show 特権レベルのコマンドには認可を設定しないことをお勧めします。

（注）　コンソール セッションから入力されたコマンドには、TACACS+ 認可は実行されません。

次の例は、*config* 特権レベルを必要とするコマンドの認可を設定する方法を示しています。最初の認可方式は TACACS+ に設定され、2 番目の認可方式はローカル ユーザ データベースに設定されています。

```
user@GUARD-conf# aaa authorization commands config tacacs+ local
```

注意　設定コマンド モードにアクセスできるようにするには、dynamic ユーザ特権レベルに対するアクセス権を付与するか、**configure** コマンドへのアクセス権を指定する必要があります。

TACACS+ サーバの設定例

TACACS+ サーバのデータベースで、各コマンドの認可を指定することができます。

例

```
user=Zoe {
    cmd = protect {
        permit .*
    }
    cmd = "no protect" {
        permit .*
    }
    cmd = learning {
        deny policy*
    }
    cmd = "no learning" {
        deny .*
    }
    cmd = dynamic-filter {
        permit .*
    }
    cmd = "no dynamic-filter" {
        permit .*
    }
    cmd = flex-filter {
        deny .*
    }
    cmd = "no flex-filter" {
        deny .*
    }
}
```

アカウンティングの設定

アカウンティング管理により、ユーザがアクセスしているサービスを追跡し、TACACS+ サーバにアカウンティング情報を保存することができます。課金、レポート、またはセキュリティの目的のため、要求されたサービスのアカウンティングをイネーブルにします。デフォルトでは、Guard モジュールのアカウンティング管理はディセーブルに設定されています。

アカウンティングを設定するには、次の手順を実行します。

ステップ 1　TACACS+ サーバ接続を設定します。詳細については、P.4-18 の「TACACS+ サーバのアトリビュートの設定」を参照してください。

ステップ 2　複数の特権レベルのアカウンティングを設定するには、アカウンティングが必要な特権レベルごとにこのコマンドを発行します。次のコマンドを入力します。

```
aaa accounting commands {show | dynamic | config | admin} stop-only
{local | tacacs+}
```

表 4-7 に **aaa accounting** コマンドのキーワードを示します。

表 4-7　aaa accounting コマンドのキーワード

パラメータ	説明
show | dynamic | config | admin	指定された特権レベルのアカウンティングを定義します（ユーザの特権レベルの詳細については、表 3-1 を参照してください）。
stop-only	コマンドの実行が終了したときにアクションを記録します。
tacacs+	アカウンティング情報の記録に TACACS+ サーバのデータベースを使用します。
local	アカウンティング情報を保存しません。

パフォーマンスへの影響を考慮し、アカウンティング管理は config ユーザ特権レベルに対してのみイネーブルにすることをお勧めします。

アカウンティング管理を削除するには、このコマンドの no 形を使用します。

次の例は、TACACS+ サーバ上で *config* 特権レベルを必要とするコマンドのアカウンティングを設定する方法を示しています。

```
user@GUARD-conf# aaa accounting commands config stop-only tacacs+
```

TACACS+ サーバのアトリビュートの設定

TACACS+ サーバのアトリビュートを設定するには、次の手順を実行します。

注意　TACACS+ 認証方式を適用する前に、TACACS+ サーバのアトリビュートを設定しておく必要があります。これを行わないと、Guard モジュールにアクセスできない場合があります。

ステップ 1　TACACS+ サーバの IP アドレスを設定します。詳細については、P.4-19 の「TACACS+ サーバの IP アドレスの設定」を参照してください。

ステップ 2　Guard モジュールが TACACS+ サーバへのアクセスに使用する暗号鍵を設定します。詳細については、P.4-20 の「TACACS+ サーバの暗号鍵の設定」を参照してください。

ステップ 3　（オプション）Guard モジュールが認証に使用する検索方式を設定します。詳細については、P.4-20 の「TACACS+ の検索の設定」を参照してください。

ステップ 4　（オプション）TACACS+ サーバの接続タイムアウトを設定します。詳細については、P.4-21 の「TACACS+ サーバの接続タイムアウトの設定」を参照してください。

ステップ 5　TACACS+ サーバ接続の統計情報を表示します。詳細については、P.4-22 の「TACACS+ サーバの統計情報の表示」を参照してください。

Guard モジュールのユーザ特権レベルは、TACACS+ の特権番号に次のように対応しています。

- admin = 15
- config = 10
- dynamic = 5
- show = 0

TACACS+ サーバの IP アドレスの設定

Guard モジュールが認証、認可、アカウンティングに TACACS+ サーバのシーケンシャルなリストを使用するように設定できます。Guard モジュールは、リストされた TACACS+ サーバを使用して、ユーザを認証または認可したり、アカウンティング イベントを送信したりします。そのサーバが応答しない場合、Guard モジュールは 2 番目のサーバを選択します。リストされたすべてのサーバを試してもうまくいかない場合、認証または認可は失敗します。

または、Guard モジュールがリストの最初の TACACS+ サーバだけを使用してユーザを認証するように設定することもできます（詳細については、P.4-20 の「TACACS+ の検索の設定」を参照）。

リストには、各 TACACS+ サーバの IP アドレスを定義する必要があります。最大 9 つの TACACS+ サーバを定義できます。

リストに TACACS+ サーバを追加し、IP アドレスを割り当てるには、設定モードで次のコマンドを入力します。

tacacs-server host *ip-address*

ip-address 引数には、TACACS+ サーバの IP アドレスを指定します。

TACACS+ サーバは、入力した順序でリストに追加されます。リストには、最大 9 つのサーバを追加できます。

例

```
user@GUARD-conf# tacacs-server host 192.168.33.45
```

TACACS+ サーバの暗号鍵の設定

TACACS+ サーバにアクセスするには、暗号鍵を設定する必要があります。コマンドの一部として入力される鍵は、TACACS+ サーバ上の鍵と一致している必要があります。鍵にスペースを含めることはできません。

サーバの暗号アクセス鍵を設定するには、設定モードで次のコマンドを入力します。

tacacs-server key *tacacs-key*

引数 *tacacs-key* は、英数字の文字列です。

（注） 定義できる暗号鍵は 1 つだけです。複数の TACACS+ サーバを使用する場合、Guard モジュールは同じ鍵を使用して、すべての TACACS+ サーバとの通信を暗号化します。

次の例は、TACACS+ サーバの暗号鍵を *TacacsKey* に設定する方法を示しています。

```
user@GUARD-conf# tacacs-server key <TacacsKey>
```

TACACS+ の検索の設定

Guard モジュールが、1 つの認証拒否を最終的なものと見なし、他の TACACS+ サーバやローカル認証方式を使用したそれ以上の検索を中止するように設定することができます。この場合、**tacacs-server first-hit** コマンドを使用します。Guard モジュールは、サーバ リストの最初の TACACS+ サーバだけを使用してユーザ認証を実行し、応答します。最初の TACACS+ サーバが応答しない場合、Guard はリストにある次のサーバを選択します。Guard は、ユーザ認証に対して最初に受け取る承認または拒否を最終的なものと見なし、他の TACACS+ サーバまたはローカル ユーザ データベースを使用したそのユーザ認証の試行を停止します。

TACACS+ の検索方式を first-hit に設定しない場合、Guard モジュールはデフォルトでリスト内のすべての TACACS+ サーバでユーザを認証しようとします。ユーザ認証として first-hit 検索方式をイネーブルにする（**no tacacs-server first-hit** コマンドを使用する）場合、Guard は、リストの最初にある TACACS+ サーバを使用してユーザを認証します。最初のサーバが応答しなかった、またはユーザの認証に失敗した場合は、Guard はリストにある次のサーバを選択します。リストにあるすべての TACACS+ サーバが応答しなかった、またはユーザ認証に失敗した場合、ローカルの認証方式が設定されていないと、そのユーザ認証は失敗します。

（注） TACACS+ の検索方式は、認証にのみ適用されます。

Guard モジュールがリストの最初の TACACS+ サーバだけを使用してユーザを認証するように設定するには、設定モードで次のコマンドを入力します。

tacacs-server first-hit

例

```
user@GUARD-conf# tacacs-server first-hit
```

TACACS+ サーバの接続タイムアウトの設定

Guard モジュールが TACACS+ サーバの応答を待つ時間を設定できます。タイムアウトが終了すると、Guard モジュールは次の TACACS+ サーバ（そのようなサーバが設定されている場合）との接続を確立しようとするか、ローカルの AAA にフォールバックします（そのようなフォールバックが設定されている場合）。フォールバックの方式が設定されていない場合、認証と認可は失敗します。

（注） すべての TACACS+ サーバとの通信に同じサーバ タイムアウトが使用されます。

TACACS+ サーバの接続タイムアウトを設定するには、設定モードで次のコマンドを入力します。

tacacs-server timeout *timeout*

timeout 引数には、Guard モジュールが TACACS+ サーバの応答を待つ時間（秒）を指定します。デフォルトのタイムアウトは 0 です。

例

```
user@GUARD-conf# tacacs-server timeout 600
```

ヒント　ネットワークに問題がある場合や、小さいタイムアウト値を使用していて、TACACS+ サーバの応答が遅いためにタイムアウトが継続的に発生する場合には、タイムアウトの値を大きくすることができます。

TACACS+ サーバの統計情報の表示

TACACS+ サーバに関連する統計情報を表示することができます。統計データは、各サーバに対して提供されます。

TACACS+ 関連の統計情報を表示するには、**show tacacs statistics** コマンドを使用します。

TACACS+ の統計情報をクリアするには、**clear tacacs statistics** コマンドを使用します。

表 4-8 に、**show tacacs statistics** コマンド出力のフィールドを示します。

表 4-8　show tacacs statistics コマンド出力のフィールドの説明

フィールド	説明
PASS	サービスが TACACS+ サーバに正常にアクセスし、アクセス権を付与された回数。
FAIL	サービスが TACACS+ サーバに正常にアクセスし、アクセス権を拒否された回数。
ERROR	サービスが TACACS+ サーバにアクセスできなかった回数。

Cisco Traffic Anomaly Detector Module との通信のイネーブル化

次のタスクをイネーブルにする場合は、Guard モジュールと Cisco Traffic Anomaly Detector Module（Detector モジュール）の間に安全な通信チャネルを確立できます。

- Remote activation of zone protection：Detector モジュールは、ゾーン トラフィックの異常を検出すると、通信チャネルを使用して Guard モジュールをアクティブにし、ゾーンを保護します。
- Synchronization of zone configuration information：Detector モジュールと Guard モジュールは、通信チャネルを介してゾーンの設定情報を交換します。

Guard モジュールは、次に示す 2 つのタイプの通信チャネルをサポートします。

- Secure Sockets Layer（SSL）：Remote activation of zone protection および Synchronization of zone configuration information をイネーブルにします。
- セキュア シェル 2（SSH2）：Remote activation of zone protection のみをイネーブルにします。

Detector モジュールは、ゾーンを保護し、ゾーンの情報を同期させるためにアクティブにする Guard モジュールのリストを保持しています。このリストは、リモート Guard リストと呼ばれます。Detector モジュールは、リモート Guard リストに設定されている各 Guard モジュールと通信チャネルを確立します。

Detector モジュールは、SSL 通信チャネルを確立する前に、各 Guard モジュールと SSH 通信チャネルを確立します。したがって、両方のタイプのリストを設定済みである場合、SSH 通信チャネルの設定を行う必要はありません。SSH 通信チャネルは SSL 通信チャネルによって設定されるためです。

この項では、次のトピックについて取り上げます。

- SSL 通信チャネルの設定
- SSH 通信チャネルの設定

SSL 通信チャネルの設定

Guard モジュールと Detector モジュールは、通信チャネルに SSL 接続を使用します。SSL は、プライバシー、認証、およびデータ整合性を組み合せることにより、接続のセキュリティを確保します。SSL の高度なセキュリティは、デジタル証明書、秘密と公開の鍵交換ペア、および Diffie-Hellman 鍵合意パラメータによって実現されます。

SSL では、デバイス認証とデータ暗号化により、安全なネットワーク通信チャネルが提供されます。それぞれの Guard モジュールと Detector モジュールは、その通信チャネルを介してデバイスと通信を試みることで、デバイスを認証します。デバイス認証は、デジタル証明書とデバイス固有の情報（IP アドレスなど）を使用して実行されます。SSL は、Guard モジュールと Detector モジュールが交換するデータを暗号化します。データを解読できるのは、指定された受信者だけです。

安全な接続を確保するために、Detector モジュールは秘密鍵と公開鍵のペアを生成し、公開鍵をリモート Guard リスト内の Guard モジュールに配布します。

Guard モジュールで通信チャネル サービスをイネーブルにした後で、Detector モジュールから通信チャネルを確立します。Detector モジュールは最初に、ユーザ *riverhead* を使用して Guard モジュールに SSH2 通信を確立します。次に Detector モジュールは、安全な SSH2 接続を使用して、SSL 接続鍵を交換します。

この項では、次のトピックについて取り上げます。

- SSL 通信チャネルの確立
- SSL 証明書の再生成

SSL 通信チャネルの確立

Guard モジュールと Detector モジュールとの間に SSL 通信チャネルを確立するには、次のタスクを実行する必要があります。

1. Guard モジュールと Detector モジュールの両方で、通信チャネル サービスをイネーブルにします。
2. Guard モジュールと Detector モジュールの両方で、その通信チャネル サービスへのアクセスを許可します。
3. Detector モジュールから通信チャネルを確立します。

Detector モジュールは最初に、ユーザ *riverhead* を使用して Guard モジュールに SSH2 通信を確立します。次に Detector モジュールは、安全な SSH2 接続を使用して、SSL 接続鍵を交換します。

注意　Guard モジュールで TACACS+ 認証を使用してユーザを認証している場合、Detector モジュールで SSH2 接続を確立するためには、TACACS+ サーバにユーザ *riverhead* を定義する必要があります。

Guard モジュールの通信チャネルをイネーブルにするには、Guard モジュール上で次の手順を実行します。

（注）　Detector モジュールの通信チャネルをイネーブルにする場合は、Detector モジュール上で同じコマンドを使用してください。

ステップ 1　Detector モジュールの IP アドレスから Guard モジュール上の SSH サービスへのアクセスを許可するため、設定モードで **permit ssh** *ip-address-general* [*ip-mask*] コマンドを入力します。

引数 *ip-address-general* および *ip-mask* を使用すると、Guard モジュールへのアクセス権を付与する対象の Detector モジュールの IP アドレスを定義できます。

（注）　SSH サービスはすでにイネーブルになっているので、ここでイネーブルにする必要はありません。

ステップ 2　通信チャネル サービスをイネーブルにするため、設定モードで **service internode-comm** コマンドを入力します。

ステップ 3　Detector モジュールの IP アドレスから通信チャネル サービスへのアクセスを許可するため、設定モードで **permit internode-comm** *ip-address-general* [*ip-mask*] コマンドを入力します。

引数 *ip-address-general* および *ip-mask* を使用すると、Guard モジュールへのアクセス権を付与する対象の Detector モジュールの IP アドレスを定義できます。

（注）　SSL 証明書内の Guard モジュールと Detector モジュールの ID は、IP アドレスに関連付けられています。通信チャネルのそれぞれの端にある Guard モジュールまたは Detector モジュールのいずれかの IP アドレスを変更する場合、SSL 証明書を再生成する必要があります。P.4-26 の「SSL 証明書の再生成」を参照してください。

SSL 証明書の再生成

SSL 証明書内の Guard モジュールと Detector モジュールを識別する鍵は、IP アドレスに関連付けられています。

次のいずれかの変更を行う場合、通信チャネルの両端にある Guard モジュールと Detector モジュール用に新しい SSL 証明書を生成する必要があります。

- いずれか一方のデバイスの IP アドレスを変更する。
- いずれか一方のデバイスを交換（スワップアウト）する。

新しい SSL 証明書を生成するには、まず、現在使用している証明書を両方のデバイスで削除する必要があります。

現在使用している SSL 証明書を消去するには、次の手順を実行します。

ステップ 1　Guard モジュールの SSL 証明書を Detector モジュールから削除します。

ステップ 2　Detector モジュールの SSL 証明書を Guard モジュールから削除します。

設定モードで次のコマンドを入力します。

```
cert remove cert-host-ip
```

cert-host-ip 引数には、Detector モジュールの IP アドレスを指定します。Guard モジュールと通信チャネルを確立したすべての Detector モジュールの SSL 証明書を削除する場合は、アスタリスク（*）を入力します。

ステップ 3　Guard　モジュールのデバイスを物理的に交換した場合は、Guard　モジュールの SSH ホスト鍵を Detector モジュールから削除する必要があります。

ステップ 4　Guard モジュールと Detector モジュールの間に新しい SSL 通信チャネルを確立します。詳細については、P.4-24 の「SSL 通信チャネルの確立」を参照してください。

次の例は、SSL 証明書を削除する方法を示しています。

```
user@GUARD-conf# cert remove 10.56.36.4
```

SSH 通信チャネルの設定

トラフィックの異常を検出すると、Detector モジュールはそのイベントをログに記録するか、SSH 接続を使用して Guard モジュールをアクティブにしてゾーンを保護します。SSH 通信チャネルを使用している場合、Detector モジュールは次のタスクを実行できません。

- ゾーン設定を同期化する。
- Guard　モジュールを監視して、ゾーンへの攻撃が終了したことを確認する。したがって、Detector モジュールを検出およびラーニングの動作状態でアクティブにしても、Detector モジュールはゾーンへの攻撃が終了したことを確認できないため、リモート Guard をアクティブにした後でゾーン トラフィックのラーニングを続行しません。

安全な SSH2 接続を確保するために、Detector モジュールは秘密 SSH 鍵と公開 SSH 鍵のペアを生成し、公開 SSH 鍵を Detector モジュールのリモート Guard リスト内の Guard モジュールに配布します。

この項では、次のトピックについて取り上げます。

- SSH 通信チャネルの確立
- SSH 通信チャネル鍵の再生成

SSH 通信チャネルの確立

Guard モジュールと Detector モジュールとの間に通信チャネルを確立するには、次のタスクを実行する必要があります。

1. Detector モジュールの IP アドレスから Guard モジュール上の SSH サービスへのアクセスを許可するため、**permit ssh** コマンドを入力します。
2. Detector モジュールから SSH 通信チャネルを確立します。

注意　Guard で TACACS+ 認証を使用してユーザを認証している場合、Detector モジュールで SSH2 接続を確立するためには、TACACS+ サーバにユーザ *riverhead* を定義する必要があります。

Guard モジュールのデバイスを交換（スワップアウト）した場合は、SSH 通信チャネルを再生成する必要があります。P.4-28 の「SSH 通信チャネル鍵の再生成」を参照してください。

SSH 通信チャネル鍵の再生成

Guard モジュールのデバイスを物理的に交換する場合、次の手順を実行して新しい SSH 通信チャネルを確立します。

ステップ 1　SSH2 ホスト鍵を Detector モジュールから削除します。設定モードにおいて、Detector モジュール上で **no host-keys** *ip-address-general* コマンドを入力します。

ip-address 引数には、リモート デバイスの IP アドレスを指定します。

Guard モジュールにリストされているホスト鍵を表示するには、**show host-keys** コマンドを使用します。

ステップ 2　次のいずれかのアクションを実行します。

- Detector モジュールから新しい SSH 通信チャネルを確立する（P.4-28 の「SSH 通信チャネルの確立」を参照）。

  または

- Detector モジュールの公開鍵をリモート Guard に手動で追加する。

  Detector モジュールの公開 SSH 鍵を表示するには、Detector モジュール上で **show public-key** コマンドを使用します。

  Detector モジュールの公開 SSH 鍵を設定するには、Guard モジュール上で **key add** コマンドを使用します。

日付と時刻の設定

時刻と日付を設定するには、設定モードで次のコマンドを入力します。

date *MMDDhhmm*[[*CC*]*YY*][.*ss*]

表 4-9 に、**date** コマンドの引数とキーワードを示します。

表 4-9　date コマンドの引数

パラメータ	説明
MM	数字で表した月。
DD	月の日付。
hh	24 時間表記の時間。
mm	分。
CC	（オプション）年の最初の 2 桁（たとえば **20**05）。
YY	（オプション）年の最後の 2 桁（たとえば 20**05**）。
.ss	（オプション）秒（小数点が必要）。

次の例は、日付を 2003 年 10 月 8 日に設定し、時刻を午後 5 時 10 分（17 時 10 分）17 秒に設定する方法を示しています。

```
user@GUARD-conf# date 1008171003.17
Wed Oct  8 17:10:17 EDT 2003
```

SSH 鍵の管理

Guard モジュールは、安全なリモート ログインのために SSH をサポートします。SSH 鍵のリストを追加すると、ログイン名とパスワードを入力せずに、リモート デバイスから Guard モジュールへの安全な通信をイネーブルにできます。

次の各項では、Guard モジュールの SSH 鍵リストの操作方法について説明します。

- SSH 鍵の追加
- SSH 鍵の削除

SSH 鍵の追加

ログイン名とパスワードを入力せずに SSH 接続をイネーブルにするには、Guard モジュールの SSH 鍵リストにリモート接続の SSH 公開鍵を追加します。

設定モードで次のコマンドを入力します。

key add [user-*name*] {**ssh-dsa** | **ssh-rsa**} *key-string comment*

表 4-10 に、**key add** コマンドの引数とキーワードを示します。

表 4-10　key add コマンドの引数とキーワード

パラメータ	説明
user-name	（オプション）指定されたユーザの SSH 鍵を追加します。他のユーザの SSH 鍵を追加できるのは管理者だけです。 デフォルトは、現行ユーザの SSH 鍵の追加です。
ssh-dsa	SSH2-DSA 鍵のタイプ。
ssh-rsa	SSH2-RSA 鍵のタイプ。
key-string	Detector またはリモート端末で作成された公開 SSH 鍵。鍵ストリングは、8,192 ビットまでに制限されています。 鍵タイプの識別（ssh-rsa または ssh-dsa）を除いた完全な鍵をコピーする必要があります。

表 4-10　key add コマンドの引数とキーワード（続き）

パラメータ	説明
comment	デバイスの説明。コメントの形式は、通常、鍵の生成に使用されるユーザとマシンを表す user@hostname になります。たとえば、Detector で生成される SSH 公開鍵に使用されるデフォルトのコメントは、**root@DETECTOR** です。

例

```
user@GUARD-conf# key add ssh-rsa 14513797528175730. . .user@Guard
module.com
```

SSH 鍵の削除

リストから SSH 鍵を削除できます。SSH 鍵を削除すると、次に Guard モジュールと SSH セッションを確立するときには認証を受ける必要があります。

Guard モジュールから SSH 鍵を削除するには、設定モードで次のコマンドを入力します。

key remove [*user-name*] *key-string*

表 4-11 で、**key remove** コマンドの引数について説明します。

表 4-11　key remove コマンドの引数

パラメータ	説明
user-name	（オプション）指定のユーザの SSH 鍵を削除します。 他のユーザの SSH 鍵を削除できるのは管理者だけです。デフォルトは、現行ユーザの SSH 鍵の削除です。
key-string	削除する公開 SSH 鍵。 プロンプトに SSH 公開鍵をペーストします。識別フィールド（ssh-rsa または ssh-dsa）は除き、鍵だけをペーストしてください。

次の例は、key remove コマンド用にカット アンド ペーストを行えるように、ユーザ鍵を表示する方法を示しています。

```
user@GUARD-conf# show keys Lilac
ssh-rsa 2352345234523456... user@Guard module.com
user@GUARD-conf# key remove Lilac 2352345234523456...
```

SFTP 接続の鍵の設定

Guard モジュールは、SSH2 の上層に位置するセキュア FTP（SFTP）をサポートします。SFTP では、公開鍵による認証と強力なデータ暗号化を使用しています。これにより、ログイン、データ、およびセッションの情報が送信中に傍受されたり変更されたりすることを防止できます。

SFTP サーバに公開鍵を設定するには、Guard モジュール上で次のアクションを実行します。

ステップ 1　Guard モジュールの公開鍵を表示します。設定モードで **show public-key** コマンドを使用します。

鍵が存在する場合は、ステップ 2 を省略し、ステップ 3 に進みます。

鍵が存在しない場合は、ステップ 2 に進みます。

ステップ 2　秘密および公開鍵ペアを生成します。設定モードで次のコマンドを入力します。

```
key generate
```

SSH の鍵ペアがすでに存在している場合は、次のメッセージが表示されます。

```
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

目的のオプションを入力します。

Guard モジュールが、公開および秘密鍵ペアを作成します。Guard モジュールの公開鍵を表示するには、設定モードで **show public-key** コマンドを使用します。

ステップ 3　公開鍵をコピーし、SFTP サーバにある鍵のファイルにペーストします。

たとえば、Linux オペレーティング システムに設置された SFTP サーバに root ユーザで接続する場合は、Guard モジュールの公開鍵を /root/.ssh/authorized_keys2 ファイルに追加します。

鍵は 1 行に収まるようにコピーしてください。鍵が 2 行としてコピーされた場合は、1 行目の末尾にある改行文字を削除します。

ホスト名の変更

Guard モジュールのホスト名を変更できます。この変更はすぐに反映され、新しいホスト名は自動的に CLI プロンプト ストリングに組み込まれます。

Guard モジュールのホスト名を変更するには、設定モードで次のコマンドを入力します。

hostname *name*

name 引数には、新しいホスト名を指定します。

例

```
user@GUARD-conf# hostname CiscoGuard
admin@CiscoGuard-conf#
```

SNMP トラップのイネーブル化

Guard モジュールが SNMP トラップを送信し、Guard モジュールで発生する重大なイベントを管理者に通知するように設定できます。Guard モジュールの SNMP トラップ ジェネレータを設定して、トラップ情報のスコープを定義することができます。

トラップのログは、Guard モジュールのイベント ログに記録され、トラップ条件が発生すると、SNMP エージェントがトラップを送信するかどうかに関係なく、イベント モニタに表示されます。

Guard モジュールが SNMP トラップを送信するように設定するには、次の手順を実行します。

ステップ 1　SNMP トラップ ジェネレータ サービスをイネーブルにします。設定モードで次のコマンドを入力します。

```
service snmp-trap
```

ステップ 2　SNMP トラップ ジェネレータ パラメータ（トラップの宛先 IP アドレスとトラップ情報のスコープ）を設定します。次のコマンドを入力します。

```
snmp trap-dest ip-address [community-string [min-severity]]
```

表 4-12 に、**snmp trap-dest** コマンドの引数を示します。

表 4-12　snmp trap-dest コマンドの引数

パラメータ	説明
ip-address	宛先ホストの IP アドレス。
community-string	（オプション）トラップとともに送信されるコミュニティ ストリング。このストリングは、宛先ホスト用に定義されたコミュニティ ストリングと一致する必要があります。デフォルトのコミュニティ ストリングは、*public* です。1 ～ 15 文字の英数字の文字列を入力します。この文字列にスペースを含めることはできません。

表 4-12　snmp trap-dest コマンドの引数（続き）

パラメータ	説明
min-severity	（オプション）トラップ情報のスコープ。重大度レベルの範囲の下限を指定してスコープを定義します。この定義により、トラップは指定された重大度レベル以上のすべてのイベントを表示します。たとえば、重大度レベル *Warnings* を指定すると、トラップは *Warnings* から *Emergencies* までのすべての重大度レベルのイベントを表示します。重大度レベルのオプションを次に示します。 • **Emergencies**：システムは使用不能（重大度 = 0） • **Alerts**：即時のアクションが必要（重大度 = 1） • **Critical**：危険な状態（重大度 = 2） • **Errors**：エラー状態（重大度 = 3） • **Warnings**：警告状態（重大度 = 4） • **Notifications**：正常ではあるが、重要な状態（重大度 =5） • **Informational**：情報通知のためのメッセージ（重大度 = 6） • **Debugging**：デバッグ メッセージ（重大度 = 7） デフォルトでは、レポートにはすべての重大度レベルのイベントが表示されます。

SNMP トラップ ジェネレータ パラメータを削除するには、**no snmp trap-dest** コマンドを使用します。すべての SNMP トラップ宛先パラメータを削除するには * を使用します。

次に、*errors* 以上の重大度レベルのトラップが、SNMP コミュニティ ストリング *tempo* とともに宛先 IP アドレス *192.168.100.52* に送信される例を示します。

```
user@GUARD-conf# snmp trap-dest 192.168.100.52 tempo errors
```

SNMP コミュニティ ストリングの設定

Guard モジュールの SNMP サーバにアクセスし、管理情報ベース 2（MIB2）および Riverhead の専用 MIB で定義された情報を取得することができます。コミュニティ ストリングはパスワードのように機能し、Guard モジュールの SNMP エージェントからの読み取りアクセスを許可します。Guard モジュールの SNMP コミュニティ ストリングを設定して、異なる組織のクライアントが異なるコミュニティ ストリングを使用して SNMP エージェントにアクセスできるようにすることができます。

SNMP コミュニティ ストリングを追加するには、設定モードで次のコマンドを入力します。

snmp community *community-string*

community-string 引数には、目的の Guard モジュールのコミュニティ ストリングを指定します。1 ～ 15 文字の英数字の文字列を入力します。この文字列にスペースを含めることはできません。Guard モジュールのデフォルトのコミュニティ ストリングは *riverhead* です。コミュニティ名はいくつでも指定できます。コミュニティ ストリングを削除するには、**no community string** コマンドを使用します。すべての SNMP コミュニティ ストリングを削除するには * を使用します。

例

```
user@GUARD-conf# snmp community tempo
```

CHAPTER 5

トラフィックの宛先変更の設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）の宛先変更プロセスについて説明します。この章は、次の項で構成されています。

- 概要
- インライン ネットワーク設定
- アウトオブパス ネットワーク設定
- トラフィック注入方式

概要

Cisco Anomaly Guard Module（Guard モジュール）は、分散型アップストリーム構成に ISP/MSP/ バックボーン レベルで配置して、ネットワーク全体を保護するための高パフォーマンス ネットワーク サービス モジュールです。

Guard モジュールは Cisco IOS アプリケーション モジュールの 1 つで、次の製品のどちらかに設置できます。

- Supervisor Engine 720（SUP720）、または Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を備えた Supervisor Engine 2（SUP2）が搭載された、Cisco Catalyst 6500 シリーズ スイッチ。Catalyst 6500 で Guard モジュールをサポートするには、IOS 12.2(18)SXD3 以降が必要です。
- SUP720 が搭載された Cisco 7600 シリーズ ルータ。7600 シリーズ ルータで Guard モジュールをサポートするには、IOS 12.2(18)SXE 以降が必要です。

攻撃が検出されると、攻撃対象ゾーンのトラフィックのみが宛先変更され、Guard モジュールに送られます。Guard モジュールは、データ フローを分析します。DDoS 要素はすべてブロックされ、宛先変更されたストリームから悪意のあるパケットが削除されます。一方、正当なトラフィックは元の宛先に転送され、継続的に目的のゾーンに流されます。

ラーニング プロセスをアクティブにすると、スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに宛先変更します。Guard モジュールは、トラフィックを分析して、保護ポリシーを作成します。その後、トラフィックをゾーンのメイン トラフィック パスに戻します（変更は加えません）。

ゾーン トラフィックを Guard モジュールに宛先変更してからメインのデータ パスに戻すサイクル全体は、宛先変更プロセスと呼ばれます。

攻撃の疑いがない場合は、宛先変更プロセスをアクティブにする必要はなく、Guard モジュールはトラフィックを監視しません。

この項では、次のトピックについて取り上げます。

- トラフィックの宛先変更
- ネットワーク設定
- 宛先変更のメカニズム

トラフィックの宛先変更

IP トラフィックの宛先変更では 2 つのタスクが実行されます。1 つまたはそれ以上のゾーンのトラフィックを Guard モジュールに宛先変更するタスクと、正当なトラフィックを Guard モジュールから元のデータ パスおよびゾーンに戻すタスクです。

宛先変更プロセスは、次の 2 つの処理で構成されています。

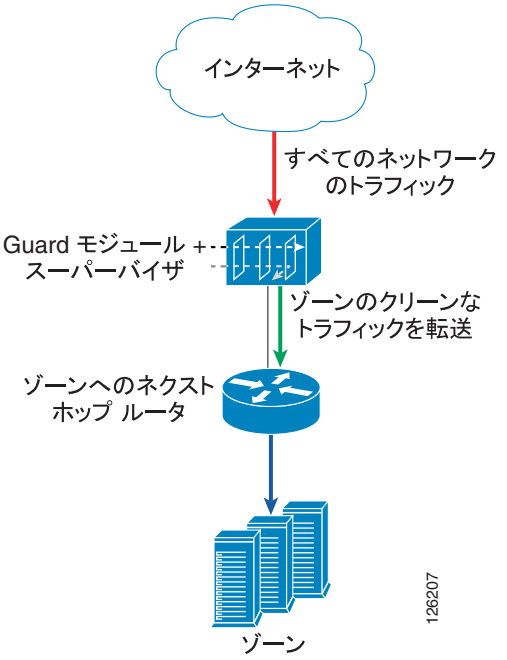
- **ハイジャック**：Guard　モジュールがゾーンを保護している場合、Guard　モジュールはゾーン トラフィックのルーティングを変更して、トラフィックが通常のスーパーバイザ エンジンのオンボード ルーティング テーブルをバイパスして Guard モジュールに流れるようにします。
- **注入**：Guard モジュールは、正当なトラフィックを元のデータ パスに戻します。

ネットワーク設定

Guard モジュールは、次のネットワーク設定のどちらかに設置できます。

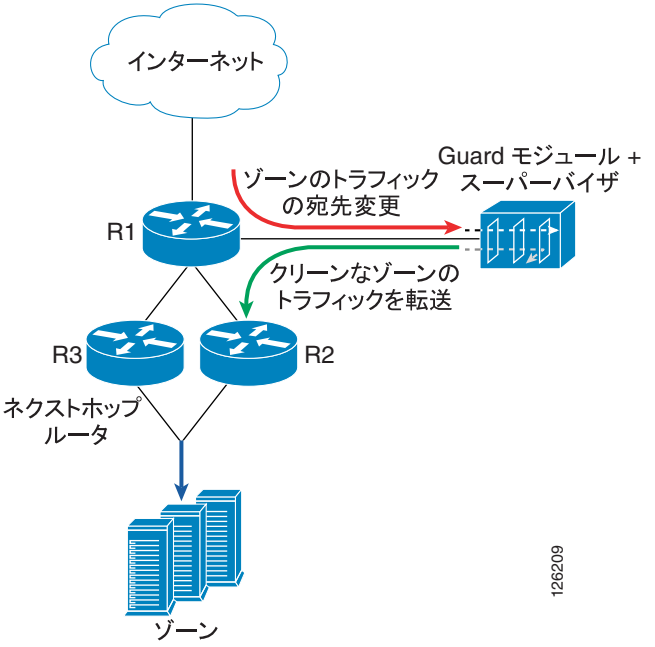
- インライン ネットワーク設定：メイン パスに存在するスイッチに Guard モジュールを設置します（つまり、ゾーン トラフィックはすでにこのスイッチを通過しています）。この設定では、Guard モジュールは、スーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加することで、ゾーン トラフィックを宛先変更します。その後、正当なトラフィックを元の宛先に再び注入します。図 5-1 に、インライン ネットワーク設定の例を示します。

図 5-1　インライン ネットワーク設定



- アウトオブパス ネットワーク設定：ゾーン トラフィックの通常のラインにあるスイッチではなく、ラインの外側にあるスイッチに Guard モジュールを設置します。この設定では、ゾーン トラフィックはゾーンの通常のラインからスイッチに宛先変更されています。ハイジャックを設定する場合、Guard モジュールはスーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加します。このスタティック ルートが BGP などの関連ルーティング プロトコルによってアドバタイズされるよう、ルーティング テーブルの再配布をあらかじめ設定しておく必要があります。図 5-2 に、アウトオブパス ネットワーク設定の例を示します。

図 5-2　アウトオブバス ネットワーク設定



宛先変更のメカニズム

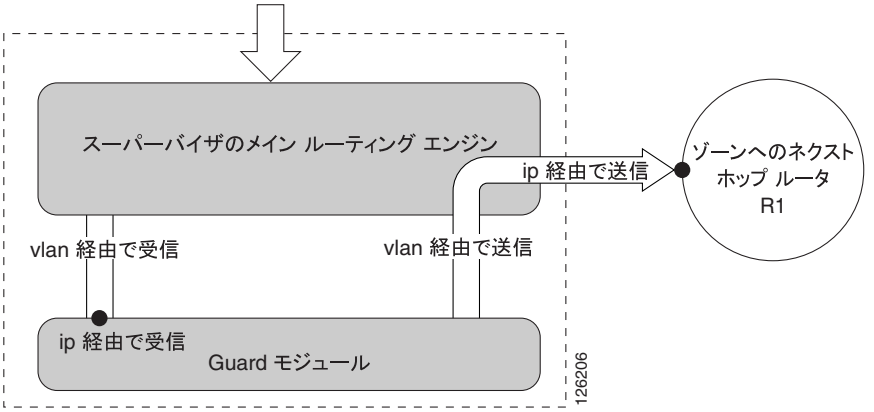
Guard モジュールの宛先変更の設定は、グローバルです。宛先変更の設定では、パケットを各サブネットにルーティングする方法を定義します。また、ハイジャックと注入の両方に必要なルートを定義します。Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合、Guard モジュールは宛先変更の設定とゾーンの定義を確認し、そのゾーンを宛先とするトラフィックを宛先変更する方法と、トラフィックをゾーンのメイン トラフィック パスに再び注入する方法を判別します。

Guard モジュールは、スーパーバイザ エンジン（RHI）に対して内部プロトコルを使用し、スーパーバイザ エンジンのオンボード ルーティング テーブルにルートを追加します。Guard モジュールは、Guard モジュールがゾーンを保護してい

る場合、またはユーザがゾーンのラーニング プロセスをアクティブにする場合にルートを追加します。ゾーン保護およびラーニング プロセスが終了すると、それらのルートは削除されます。

図 5-3 に、スーパーバイザ エンジンのオンボード ルーティング テーブルと Guard モジュールの間でパケットをルーティングする方法を図示します。

図 5-3　　宛先変更のメカニズム



（注） トラフィックのハイジャックと注入には、同じ VLAN を設定できます。

ハイジャックと注入のパラメータは、システム管理者が設定できます。

この項では、次のトピックについて取り上げます。

- ハイジャック パラメータ
- 注入パラメータ
- 宛先変更ルートの表示

ハイジャック パラメータ

ゾーンの保護をアクティブにすると、スーパーバイザ エンジンのオンボード ルーティング エンジンが、ゾーン トラフィックを Guard モジュールに宛先変更します。スーパーバイザ エンジンから Guard モジュールへのトラフィックは、VLAN *receive-via-vlan* に宛先変更されます。Guard モジュールは IP アドレス *receive-via-ip* を使用して、この VLAN でゾーン トラフィックを受信します。トラフィックのハイジャックと注入の両方には、同じ VLAN を使用できます。

Guard モジュールは、スーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートをインストールします。このとき、ゾーン トラフィックが Guard モジュールに確実に宛先変更されるよう、ゾーンへのネクストホップとして Guard モジュールを指します。Guard モジュールは、最長プレフィクスの照合アルゴリズムを使用します。つまり、各ルートをより長いプレフィクスを持つ 2 つのルートに分割し、これらのルートをスーパーバイザ エンジンのオンボード ルーティング テーブルにアドバタイズします。たとえば、24 ビット長のゾーン サブネット（クラス C）のルートは、25 ビット長のゾーン サブネットの 2 つのルートとして発行されます。

複数のハイジャック ルートを追加できます。各ハイジャック ルートは、ルート プリファレンスを定義する重みを持ちます。スーパーバイザ エンジンのオンボード ルーティング エンジンは、最大の重みを持つパスを優先的に使用します。デフォルトでは、すべてのハイジャック ルートに重みとして 1 が追加されています。デフォルトの重みを変更して、複数のハイジャック ルート間のプリファレンスを定義することができます。

ハイジャック パラメータを注入ルートに関連付けることができます。または、グローバルなハイジャック パラメータを設定することもできます。

（注） ハイジャック パラメータを入力しない場合は、Guard モジュールがパラメータを動的に設定します。VLAN ID 値は、Guard モジュールのインターフェイス *giga2* に定義された VLAN ID に動的に設定され、*receive-via-ip* はその VLAN の IP アドレスに設定されます。VLAN が定義されていない場合、VLAN ID は *1* に設定され、*receive-via-ip* は *giga2* インターフェイスの IP アドレスに設定されます。

ハイジャック パラメータを注入ルートに関連付ける方法については、次の項、「注入パラメータ」を参照してください。

グローバルなハイジャック パラメータを設定するには、次のコマンドを入力します。

diversion hijacking {**receive-via-ip** *receive-via-ip* | **receive-via-vlan** *receive-via-vlan* | **weight** *weight*}

表 5-1 で、**diversion hijacking** コマンドの引数について説明します。

表 5-1　diversion hijacking コマンドの引数

パラメータ	説明
receive-via-ip	スーパーバイザ エンジンがゾーン トラフィックを転送する Guard モジュールの IP アドレス。
receive-via-vlan	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときに使用される VLAN。
weight	宛先変更ハイジャック ルートの重み。デフォルト値は 1 です。

デフォルト値を復元する場合は、**no diversion hijacking** コマンドを使用します。

注入パラメータ

Guard モジュールは、宛先変更されたストリームから悪意のあるパケットを削除し、正当なトラフィックを、スーパーバイザ エンジンのオンボード ルーティング エンジン（レイヤ 3）に戻すか、またはゾーンのメイン トラフィック パス（レイヤ 2）に直接戻します。正当なトラフィックは VLAN *send-via-vlan* 上で送信されます。レイヤ 2 注入の場合は、ネクストホップ ルータと Guard モジュールが同じ VLAN 上に存在する必要があります。レイヤ 2 でゾーンのメイン トラフィック パスにトラフィックを注入するには、ゾーンへのネクストホップがネクストホップ ルータの IP アドレスになるように設定します。

注意　L2 注入を設定する場合は、ネクストホップ ルータとしてスーパーバイザ エンジンの IP アドレスを入力しないでください。このように入力すると、ルーティング ループが発生する場合があります。

注入パラメータを設定するには、次のコマンドを入力します。

diversion injection *ip-address ip-mask* **nexthop** *next-hop*

ip-address および *ip-mask* 引数にはゾーンの IP アドレスを指定し、*next-hop* 引数にはネクストホップ ルータの IP アドレスを指定します。

IP アドレスとサブネット マスクは、特定のゾーンのものと一致する必要はありません。これらは、ゾーン定義のサブセットにすることも、複数のゾーンのサブセットにすることもできます。たとえば、1 つまたは 2 つのコマンドを使用して、候補となる数百ものゾーンのネットワークについて宛先変更を設定することができます。

ハイジャック パラメータを注入ルートに関連付けることができます。または、グローバルなハイジャック パラメータを設定することもできます。

ハイジャック パラメータを注入ルートに関連付けるには、次のコマンドを入力します。

diversion injection *ip-address ip-mask* **nexthop** *next-hop* [**hijacking** [**receive-via-ip** *receive-via-ip*] [**receive-via-vlan** *receive-via-vlan*] [**weight** *weight*]]

ip-address および *ip-mask* 引数にはゾーンの IP アドレスを指定し、*next-hop* 引数にはネクストホップ ルータの IP アドレスを指定します。ハイジャック パラメータについては、前の項、「ハイジャック パラメータ」を参照してください。

宛先変更ルートの表示

Guard モジュールは、RHI メッセージを使用して、スーパーバイザ エンジンのオンボード ルーティング テーブルを変更します。Guard モジュールは、Guard モジュールがゾーンを保護している場合、またはユーザがゾーンのラーニング プロセスをアクティブにする場合にルートを追加します。ゾーン保護およびラーニング プロセスが終了すると、それらのルートは削除されます。

Guard モジュールの宛先変更の設定を表示するには、**show diversion** コマンドを使用します。

このメッセージは、Guard モジュールがゾーンを保護しているとき、またはゾーンがラーニング プロセス中のときに、スーパーバイザ エンジン上に表示できます。

Guard モジュールがアドバタイズしたルートを表示するには、スーパーバイザ エンジンで次のコマンドを入力します。

show anomaly-guard module *module_number* **advertised-route**

module_number 引数には、モジュールが装着されているスロットの番号を指定します。

例

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9
    ip              mask            nexthop          vlan    weight
    --------------  --------------- ---------------  ------ ------
A   192.168.252.8   255.255.255.0  192.168.8.10     8       1
```

Guard がスタティック ルートを追加したことを確認するには、スーパーバイザ エンジンのオンボード ルーティング テーブルを表示します。

スーパーバイザ エンジンで次のコマンドを入力します。

show ip route

例

```
Sup# show ip route
C    192.168.8.0/24 is directly connected, Vlan8
S    192.168.252.8/32 [1/0] via 192.168.8.10, Vlan8
.
.
.
```

インライン ネットワーク設定

インライン ネットワーク設定では、Guard モジュールはゾーンのクリティカル パスに常駐するスイッチに設置されます。つまり、ゾーンが Guard モジュールによって保護されかどうかに関係なく、ゾーン トラフィックはこのスイッチを通過します。

この項では、次のトピックについて取り上げます。

- ハイジャック
- 注入
- インラインの宛先変更の設定

ハイジャック

宛先変更を設定する場合、Guard モジュールは RHI メッセージを使用して、スーパーバイザ エンジンのオンボード ルーティング テーブルにルートを追加します。Guard モジュールは、ゾーン トラフィックが Guard モジュールに必ず直接転送されるよう、最も長くプレフィックスが一致するルートを追加します。次に、データ フローを分析します。宛先変更されたストリームから悪意のあるパケットをすべて削除し、注入メカニズムを使用して、正当なトラフィックを元の宛先に戻します。その結果、トラフィックは継続的に目的のゾーンに流されます。

注入

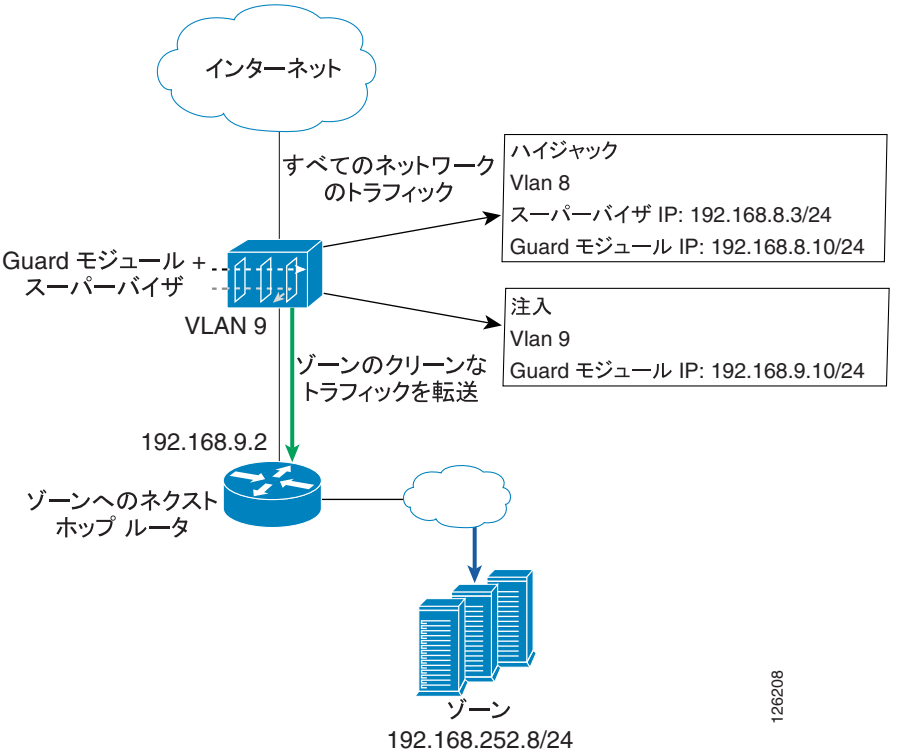
正当なトラフィックを元の宛先に戻す場合は、レイヤ 2 またはレイヤ 3 のトラフィック注入方式を使用できます。詳細については、P.5-23 の「トラフィック注入方式」を参照してください。

インラインの宛先変更の設定

図 5-4 に、インライン ネットワーク設定におけるトラフィック宛先変更の例を示します。この例では、レイヤ 3 でハイジャックが、レイヤ 2 で注入が実行されています。

(注)　宛先変更を設定する前に、ネットワークを設定する必要があります。詳細については、第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」および第 3 章「Guard モジュールの初期化」を参照してください。

図 5-4　インライン ネットワーク設定（L3 トポロジ）の例



- Guard モジュールは、スイッチのスロット 9 に設置されている。
- スイッチ上のポート GigabitEthernet2/2 は、VLAN 9 でネクストホップ ルータに接続されている。

次に、スーパーバイザ エンジンと Guard モジュールを設定する方法を、設定例とともに示します。

ステップ 1　スーパーバイザ エンジンでスイッチ インターフェイスを設定します。次のコマンドを入力します。

```
Sup# conf term
Sup(config)# vlan 8,9
Sup(config)# anomaly-guard module 9 port 2 allowed-vlan 8,9
Sup(config)# interface vlan 8
Sup(config-if)# ip address 192.168.8.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface vlan 9
Sup(config-if)# ip address 192.168.9.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface GigabitEthernet2/2
Sup(config-if)# switchport
Sup(config-if)# switchport mode access
Sup(config-if)# switchport access vlan 9
```

ステップ 2　Guard モジュールで Guard モジュールのインターフェイスを設定します。次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# interface giga 2
user@GUARD-conf-if-giga2# no shutdown
user@GUARD-conf-if-giga2# exit
user@GUARD-conf# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.89# exit
user@GUARD-conf#interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# exit
```

ステップ 3　Guard モジュールで宛先変更を設定します。次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-ip 192.168.8.10
user@GUARD-conf# diversion hijacking receive-via-vlan 8
user@GUARD-conf# diversion injection 192.168.252.0 255.255.255.0
nexthop 192.168.9.2
```

ステップ 4　**protect** コマンドまたは **learning** コマンドを発行してゾーンをアクティブにしたら、Guard モジュールがアドバタイズしたルートと、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示できます。

Guard モジュールがアドバタイズしたルートを表示するには、**show anomaly-guard module advertised-route** コマンドを使用します。スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示するには、**show ip route** コマンドを使用します。

次の例は、Guard モジュールがスーパーバイザ エンジンにアドバタイズしたルートを表示する方法を示しています。

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9

    ip              mask           nexthop          vlan    weight
    --------------  -------------- ---------------  ------ ------
A   192.168.252.0   255.255.255.128192.168.8.10     8       1
A   192.168.252.128 255.255.255.128192.168.8.10     8       1
```

（注）　Guard モジュールは、Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合にこれらのルートをアドバタイズします。アドバタイズされたルートを表示するには、ゾーンが現在ラーニング プロセス中であること、または Guard モジュールがゾーンを保護していることを確認します。

次の例は、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示する方法を示しています。

```
Sup# show ip route
...
192.168.252.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.168.252.0/25 [1/0] via 192.168.8.10, Vlan8
S       192.168.252.128/25 [1/0] via 192.168.8.10, Vlan8
```

アウトオブパス ネットワーク設定

アウトオブパス ネットワーク設定では、Guard モジュールは、ゾーン トラフィックの通常のラインにあるスイッチではなく、ラインの外側にあるスイッチに設置されます。この設定では、ゾーン トラフィックはゾーンの通常のラインからスイッチに宛先変更されています。

この項では、次のトピックについて取り上げます。

- ハイジャック
- 注入
- アウトオブパスの宛先変更の設定

ハイジャック

宛先変更を設定する場合、Guard モジュールは RHI メッセージを使用して、スーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加します。Guard モジュールは、ゾーン トラフィックが Guard モジュールに必ず直接転送されるよう、最も長くプレフィックスが一致するルートを追加します。BGP などの関連ルーティング プロトコルがこのスタティック ルートをアドバタイズするよう、ルーティング テーブルの配布をあらかじめ設定しておく必要があります。

Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合、Guard はスーパーバイザ エンジンのオンボード ルーティング テーブルを変更します。ゾーン トラフィックが宛先変更されたルータ（宛先変更元ルータ）に BGP（EBGP または IBGP）アナウンスメントを発行するように、スーパーバイザ エンジンまたは MSFC を設定する必要があります。この BGP アナウンスメントに基づいて、宛先変更元ルータはそのルーティング テーブルを変更します。アナウンスメントにより、特定のゾーンへの最適なネクストホップとして Guard がリストされます。Guard モジュールの隣接ルータがアナウンスメントを転送しないことを保証するには、*no-advertise* と *no-export* の BGP コミュニティ ストリングを設定します。したがって、ゾーンを宛先とするパケットがネクストホップ ルータに到達すると、ルータはそのパケットをゾーンに転送します（Guard モジュールには戻しません）。

注入

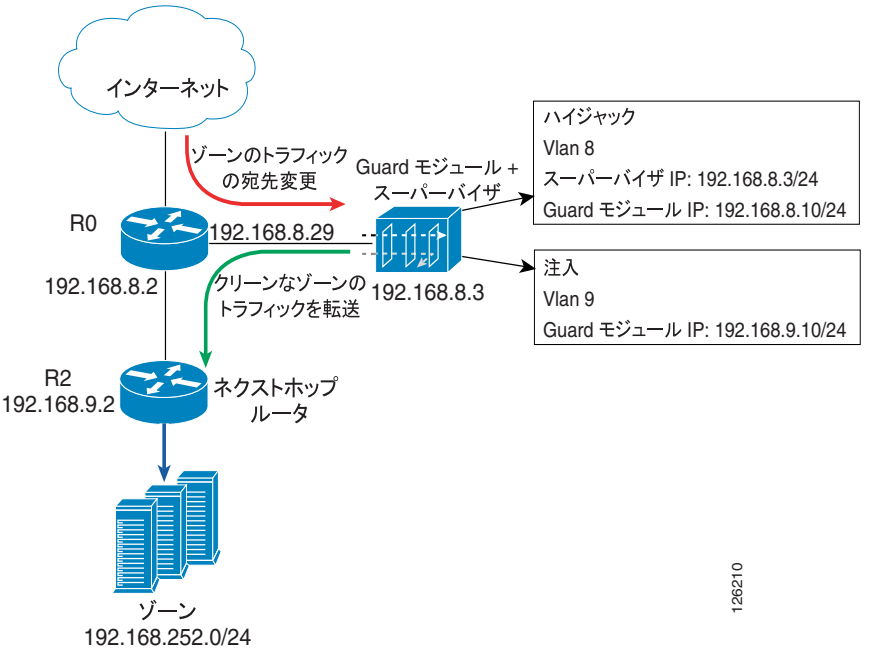
正当なトラフィックを元の宛先に戻す場合は、レイヤ 2 またはレイヤ 3 のトラフィック注入方式を使用できます。詳細については、P.5-23 の「トラフィック注入方式」を参照してください。

アウトオブパスの宛先変更の設定

図 5-4 に、アウトオブパス ネットワーク設定におけるトラフィック宛先変更の例を示します。この例では、レイヤ 3 でハイジャックが、レイヤ 2 で注入が実行されています。

（注） 宛先変更を設定する前に、ネットワークを設定する必要があります。詳細については、第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」および第 3 章「Guard モジュールの初期化」を参照してください。

図 5-5　アウトオブパス ネットワーク設定（L3 トポロジ）の例



- Guard モジュールは、スイッチのスロット 9 に設置されている。
- スイッチ上のポート GigabitEthernet2/2 は、VLAN 9 でネクストホップ ルータに接続されている。
- R0 と R2 は Autonomous System（AS; 自律システム）100 に存在し、Guard モジュールは AS 55 に存在する。

（注） Guard モジュールがゾーンを保護している場合、トラフィックは R0 から R2 に直接流れます。ゾーン トラフィックのルートは、大きな（1 より大きい）重みを持つか、Guard モジュールが持つルートよりも限定的でないルートを持つ必要があります。

次に、スーパーバイザ エンジンと Guard モジュールを設定する方法を、設定例とともに示します。

ステップ 1　スーパーバイザ エンジンでスイッチ インターフェイスを設定します。次のコマンドを入力します。

```
sup# conf term
Sup(config)# vlan 8,9
Sup(config)# anomaly-guard module 9 port 2 allowed-vlan 8,9
Sup(config)# interface vlan 8
Sup(config-if)# ip address 192.168.8.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface vlan 9
Sup(config-if)# ip address 192.168.9.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface GigabitEthernet2/2
Sup(config-if)# switchport mode trunk
Sup(config-if)# switchport trunk encapsulation dot1q
Sup(config-if)# switchport
Sup(config-if)# switchport access vlan 9
Sup(config-if)# switchport mode access
```

ステップ 2　Guard モジュールがスーパーバイザ エンジンのオンボード ルーティング テーブルに追加するスタティック ルートだけが隣接ルータに発行されるよう、スーパーバイザ エンジンにルート マップを設定します。*no-advertise* と *no-export* の BGP コミュニティ ストリングを設定します。

次のコマンドを入力します。

```
sup# conf term
Sup(config)# access-list 61 permit 192.168.8.10
Sup(config)# route-map PERMIT_GUARD_ONLY permit 10
Sup(config-route-map)# match ip next-hop 61
Sup(config-route-map)# set community no-export no-advertise
Sup(config-route-map)# exit
Sup(config)# route-map PERMIT_GUARD_ONLY deny 20
```

ステップ 3　スーパーバイザ エンジンに BGP 再配布ルートを設定します。AS 100 の隣接ルータを定義します。スーパーバイザ エンジンが Guard モジュールの *receive-via-ip* アドレスに等しい宛先 IP アドレスを使用してオンボード ルーティング テーブルにスタティック ルートを追加するたびに BGP アナウンスメントを発行するように、スーパーバイザ エンジンを設定します。

次のコマンドを入力します。

```
sup# conf term
Sup(config)# router bgp 55
Sup(config-router)# bgp log-neighbor-changes
Sup(config-router)# neighbor 192.168.8.29 remote-as 100
Sup(config-router)# address-family ipv4
Sup(config-router-af)# redistribute static route-map PERMIT_GUARD_ONLY
Sup(config-router-af)# neighbor 192.168.8.29 activate
Sup(config-router-af)# no auto-summary
Sup(config-router-af)# no synchronization
Sup(config-router-af)# exit-address-family
```

ステップ 4　Guard モジュールで Guard モジュールのインターフェイスを設定します。次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# exit
user@GUARD-conf# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# exit
```

ステップ 5　Guard モジュールで宛先変更を設定します。次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-ip 192.168.8.10
user@GUARD-conf# diversion hijacking receive-via-vlan 8
user@GUARD-conf# diversion injection 192.168.252.0 255.255.255.0
nexthop 192.168.9.2
```

ステップ 6　ルータ R0 に BGP 設定値を設定します。次のコマンドを入力します。

```
RouterR0# conf term
RouterR0(config)# router bgp 100
RouterR0(config-router)# neighbor 192.168.8.3 remote-as 55
```

ステップ 7　**protect** コマンドまたは **learning** コマンドを発行してゾーンをアクティブにしたら、Guard モジュールがアドバタイズしたルートと、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートをスーパーバイザ エンジン上に表示できます。

Guard モジュールがアドバタイズしたルートを表示するには、**show anomaly-guard module advertised-route** コマンドを使用します。スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示するには、**show ip route** コマンドを使用します。

次の例は、Guard モジュールがアドバタイズしたルートを表示する方法を示しています。

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9

    ip              mask           nexthop          vlan    weight
    --------------  -------------- ---------------  ------ ------
A   192.168.252.8   255.255.255.0  192.168.8.10     8       1
```

（注）　Guard モジュールは、ゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合にこれらのルートをアドバタイズします。アドバタイズされたルートを表示するには、ゾーンが現在ラーニング プロセス中であること、または Guard モジュールがゾーンを保護していることを確認します。

次の例は、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示する方法を示しています。

```
Sup# show ip route
...
192.168.252.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.168.252.0/25 [1/0] via 192.168.8.10, Vlan8
S       192.168.252.128/25 [1/0] via 192.168.8.10, Vlan8
```

ステップ 8　ルータ R0 がゾーンへの新しいルート（Guard モジュールによってアドバタイズされたもの）をルーティング テーブルに追加したことを確認します。ルータ R0 上の BGP ルーティング テーブルを表示します。

次の例は、Guard モジュールがゾーンへの新しいルートをアドバタイズする前の BGP ルーティング テーブルを示しています。

```
RouterR0# show ip bgp
.
.
.
    Network          Next Hop       Metric LocPrf    Weight  Path
*>  192.168.252.0/24192.168.9.2    0                0       100 ?
```

次の例は、Guard モジュールがゾーンへの新しいルートをアドバタイズした後の BGP ルーティング テーブルを示しています。

```
RouterR0# show ip bgp
.
.
.
    Network          Next Hop       Metric LocPrf    Weight  Path
*>  192.168.252.0/25192.168.8.3    0                0       55 ?
*>  192.168.252.128/25192.168.8.3  0                0       55 ?

RouterR0#
```

トラフィック注入方式

この項では、Guard モジュールからネクストホップ ルータに正当なトラフィックを注入する際に使用される各方式について説明します。方式は、2 つのメイン ネットワーク トポロジによって異なります。

- レイヤ 2 トポロジ
- レイヤ 3 トポロジ

レイヤ 2 トポロジ

このトポロジでは、正当なトラフィックを元の宛先に戻すために、Guard モジュールが正当なトラフィックをネクストホップ ルータに直接転送します。スーパーバイザ エンジンがルーティングを決定する必要はありません。

Guard モジュールは、ネクストホップ ルータの IP アドレスに ARP クエリーを送信して、ネクストホップ ルータの MAC アドレスを特定します（詳細については、P.5-8 の「注入パラメータ」を参照）。次に、関連するネクストホップ ルータに接続されているスイッチ インターフェイスに正当なトラフィックを転送します。したがって、スーパーバイザ エンジンとゾーンへのネクストホップ ルータは同じ VLAN 上に存在する必要があり、Guard モジュールはその VLAN 上に IP アドレスを持っている必要があります。

設定例については、P.5-12 の「インラインの宛先変更の設定」および P.5-17 の「アウトオブパスの宛先変更の設定」を参照してください。

レイヤ 3 トポロジ

このトポロジでは、正当なトラフィックを元の宛先に再び注入するために、スーパーバイザ エンジンがルーティングを決定する必要があります。Guard モジュールは、正当なトラフィックを次の宛先のどちらかに注入できます。

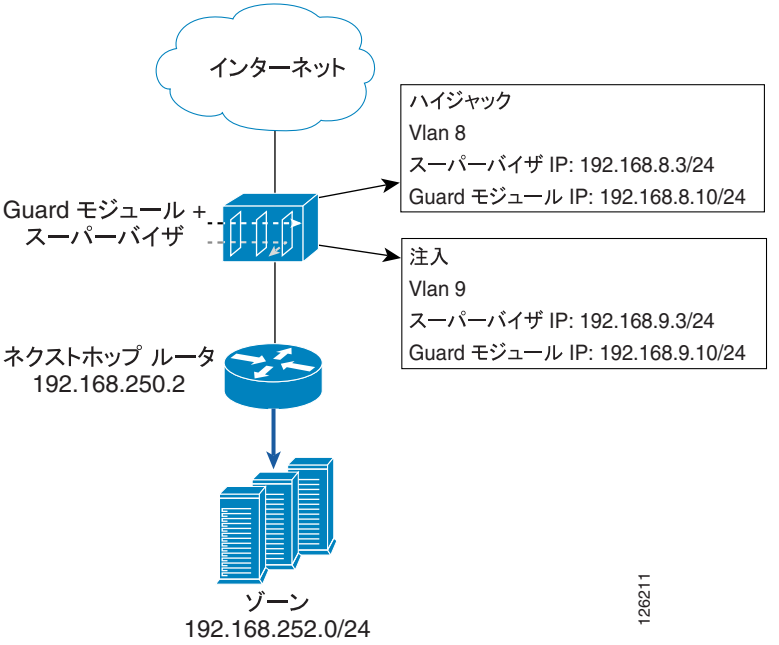
- 別のルータまたは VLAN：設定例については、P.5-12 の「インラインの宛先変更の設定」を参照してください。
- トラフィックの宛先変更元。

protect コマンドまたは **learning** コマンドを発行してゾーンをアクティブにする場合、Guard モジュールは、ゾーンへの最良のパスとしてリストされるようにルーティング テーブルを変更します（ルーティング テーブルは、ネットワーク トポロジに応じて、スーパーバイザ エンジンのオンボード ルーティング テーブルまたは隣接ルータのルーティング テーブルのどちらかです）。Guard モジュールが正当なトラフィックをトラフィックの宛先変更元に戻す場合、ルーティング ループが発生することがあります。そのようなルーティング ループが発生しないようにするには、ルーティング規則を Guard モジュールがゾーンに転送する正当なトラフィックに関連付けます。この規則は、グローバルなルーティング テーブルを上書きするように設定できます。

VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）ルーティング インスタンスを使用すると、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加の転送テーブルを作成できます。この方式を使用すると、スーパーバイザ エンジンのオンボード ルーティング テーブルを使用せずにトラフィックを転送できるため、ルーティング ループを回避できます。この転送テーブルを使用して、Guard モジュールからゾーンに送信されるパケットをルーティングするための代替注入パスを定義します。転送テーブルには、ゾーンへのネクストホップ ルータにトラフィックを転送する方法についての情報だけを含めます。

ゾーン トラフィックは、ネクストホップ ルータに直接転送するか、トンネルに注入することができます。

図 5-6　　レイヤ 3 注入の設定例



この項では、次のトピックについて取り上げます。

- VRF の設定

VRF の設定

VRF は、レイヤ 3 ネットワーク トポロジで展開される注入方式です。この方式では、Guard モジュールが、正当なトラフィックをトラフィックのハイジャック元のルータに再び注入します。VRF は、インライン ネットワーク設定とアウトオブパス ネットワーク設定の両方に適用できます。

VRF を使用すると、グローバルなルーティング / 転送テーブルのほかに、もう 1 つルーティング / 転送テーブル（VRF テーブルと呼ばれる）を作成できます。このテーブルは、Guard モジュールとのインターフェイス上で受信されるトラフィックをルーティングするように設定します。

（注） 設定は、インライン ネットワーク設定とアウトオブパス ネットワーク設定の両方に適用されます。

次の 2 つのインターフェイスを設定します。

- **ハイジャック　インターフェイス**：このインターフェイスは、トラフィックを Guard モジュールに宛先変更する場合に使用します。この VLAN 上のトラフィックは、グローバル ルーティング テーブルに従って転送されます。次の例では、ハイジャック用に VLAN 8 を使用します。
- **注入インターフェイス**：このインターフェイスは、戻されたトラフィックを Guard モジュールからゾーンのメイン データ パスに注入する場合に使用します。このインターフェイスに VRF テーブルを設定します。VRF テーブル内のスタティック ルートは、Guard モジュールからゾーンに送信されたすべてのトラフィックをネクストホップ ルータに転送するように設定します。次の例では、注入用に VLAN 9 を使用します。

  トラフィックは、次の方式のどちらかを使用して注入できます。

  — 直接注入

  — トンネルを介した注入

（注） 複数のネクストホップ ルータを設定できます。

この項の設定は、図 5-6 のネットワーク設定に適用されます。Guard モジュールは、スイッチのスロット 9 に設置されています。

次に、スーパーバイザ エンジンと Guard モジュールを設定する方法を、設定例とともに示します。

ステップ 1　スーパーバイザ エンジン上に VRF テーブルを作成します。次のコマンドを入力します。

```
Sup# conf term
Sup(config)# ip vrf Guard-vrf
Sup(config-vrf)# rd 100:1
```

ステップ 2　スーパーバイザ エンジンに VRF テーブルを設定します。トラフィックの注入は、次の方式のどちらかを使用して設定できます。

- トラフィックをネクストホップ　ルータに直接注入する。詳細については、P.5-28 の「直接注入」を参照してください。
- トンネルを介してトラフィックを注入する。詳細については、P.5-29 の「トンネルを介した注入」を参照してください。

ステップ 3　スーパーバイザ エンジンに VLAN インターフェイスを設定し、このインターフェイスを Guard モジュールに関連付けます。次のコマンドを入力します。

```
Sup# conf term
Sup(config)# interface vlan 8
Sup(config-if)# ip address 192.168.8.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no ip directed-broadcast
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface vlan 9
Sup(config-if)# ip vrf forwarding Guard-vrf
Sup(config-if)# ip address 192.168.9.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# anomaly-guard module 9 port 2 allowed-vlan 8,9
```

ステップ 4　Guard モジュールで Guard モジュールのインターフェイスを設定します。次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# exit
user@GUARD-conf# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# exit
```

ステップ 5　Guard モジュールで宛先変更を設定します。次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-ip 192.168.8.10
user@GUARD-conf# diversion hijacking receive-via-vlan 8
user@GUARD-conf# diversion injection 192.168.252.0 255.255.255.0
nexthop 192.168.9.3
```

直接注入

ゾーンへのルートを指定するには、VRF テーブルにスタティック ルートを追加します。**global** キーワードは、ネクストホップ ルータへのルートがグローバル ルーティング テーブルからラーニングされることを示します。スーパーバイザ エンジンで次のコマンドを入力します。

```
Sup(config)# ip route vrf Guard-vrf 192.168.252.0 255.255.255.0
192.168.250.2 global
```

または、VRF ごとに特定のルーティング プロトコル インスタンスを定義することもできます。たとえば、**address-family ipv4 vrf** コマンドを使用すると、VRF の特定の BGP インスタンスを作成できます。

トンネルを介した注入

トンネルを介した注入を設定するには、次の手順を実行します。

ステップ 1　スーパーバイザ エンジンにトンネルを設定します。次のコマンドを入力します。

（注）　次の例では、GRE トンネルを使用します。

```
Sup# conf term
Sup(config)# interface tunnel5
Sup(config-if)# ip address 192.168.145.2 255.255.255.252
Sup(config-if)# tunnel source 192.168.8.3
Sup(config-if)# tunnel destination 192.168.7.1
```

ステップ 2　ネクストホップ ルータにトンネル側を設定します。次のコマンドを入力します。

```
router# conf term
router(config)# interface tunnel5
router(config-if)# ip address 192.168.145.1 255.255.255.252
router(config-if)# tunnel source 192.168.7.1
router(config-if)# tunnel destination 192.168.8.3
```

ステップ 3　ゾーンへのルートを指定するスーパーバイザ エンジンの VRF テーブルに、スタティック ルートを追加します。**global** キーワードは、ネクストホップ ルータへのルートがグローバル ルーティング テーブルからラーニングされることを示します。次のコマンドを入力します。

```
Sup(config)# ip route vrf Guard-vrf 192.168.252.0 255.255.255.0
192.168.145.1 global
```

CHAPTER 6

ゾーンの設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）上でゾーンを作成し、管理する方法について説明します。これらの手順は、ゾーン保護をイネーブルにするために必要です。

この章には、次の項があります。

- 概要
- ゾーンの作成
- ゾーンのアトリビュートの設定
- ゾーン トラフィックの特性のラーニング
- ゾーン ポリシーのしきい値の調整とゾーン保護のイネーブル化の同時実行
- Guard モジュールのゾーン設定と Detector モジュールの同期
- ゾーンの保護
- オンデマンド保護のイネーブル化

概要

ゾーンは、Guard で DDoS 攻撃からの保護の対象となるネットワーク要素です。ゾーンは、ネットワーク サーバ、クライアント、ルータ、ネットワーク リンク、サブネット、ネットワーク全体、個々のインターネット ユーザ、企業、インターネット サービス プロバイダー（ISP）、またはこれらを組み合せたものを包含できます。Guard は、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンを同時に保護できます。

ゾーンには、名前を割り当て、この名前を使用してゾーンを参照します。

ゾーンの設定処理には、次のタスクがあります。

- ゾーンの作成：ゾーンを作成し、ゾーン名、説明、およびネットワーク IP アドレスなど、ゾーンのアトリビュートを設定します。詳細については、P.6-3 の「ゾーンの作成」を参照してください。
- ゾーン フィルタの設定：さまざまなゾーン フィルタを設定します。ゾーン フィルタは、ゾーン トラフィックを必要な保護レベルに誘導し、Guard モジュールが特定のトラフィック フローを処理する方法を定義します。詳細については、第 7 章「ゾーンのフィルタの設定」を参照してください。
- ゾーンのトラフィック特性のラーニング：Guard モジュールが特定のトラフィック フローを分析し、トラフィック フローがポリシーのしきい値を超過した場合にアクションを実行することを可能にする、ゾーンの保護ポリシーを作成します。ポリシーは、ポリシー構築およびしきい値調整という 2 つのフェーズで構成されるラーニング プロセスの中で構築されます。詳細については、P.6-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。

ゾーンの作成

ゾーンを作成し、ゾーンのアトリビュートを設定します。ゾーンのアトリビュートは、ゾーン名、ゾーンの説明、ゾーンのネットワーク アドレス、ゾーンの動作定義、およびネットワーク定義で構成されています。

新しいゾーンを作成するときには、既存のゾーンをテンプレートとして使用するか、またはシステム定義のゾーン テンプレートからゾーンを作成することができます。ゾーン テンプレートには、ゾーンの初期ポリシーおよびフィルタ設定が定義されています。

新しいゾーンには、オンデマンド保護用に調整されたデフォルト ポリシーが割り当てられます。ただし、すぐにゾーンを保護する必要がない場合は、Guard モジュールでゾーンのトラフィック特性をラーニングすることをお勧めします。詳細については、P.6-45 の「オンデマンド保護のイネーブル化」を参照してください。または、ゾーンの設定とゾーン ポリシーを Detector モジュールからコピーすることもできます。

新しいゾーンは、次の 3 つの方法で作成できます。

- 新しいゾーンの作成：システム定義のゾーン　テンプレートから新しいゾーンを作成します。この方式は、デフォルトのポリシーおよびフィルタを使用して新しいゾーンを作成する場合に使用します。

  新しいゾーンを作成したら、ゾーンの特性を設定する必要があります。
- ゾーンの複製：既存のゾーンからゾーンを作成します。この方式は、新しいゾーンに既存のゾーンと同様のトラフィック パターンを割り当てる場合に使用します。
- Detector モジュールからのゾーン設定のコピー：この方式は、ゾーン設定と Detector モジュールの同期をイネーブルにする場合に使用します。P.6-30 の「Guard モジュールのゾーン設定と Detector モジュールの同期」を参照してください。

  このアクションは、Cisco Traffic Anomaly Detector Module だけで開始できます。詳細については、『*Cisco Trafiic Anomaly Detector Module Configuration Guide*』を参照してください。

ゾーン設定の設定値を変更する方法については、P.6-9 の「ゾーンのアトリビュートの設定」を参照してください。

新しいゾーンの作成

システム定義のゾーン テンプレートから新しいゾーンを作成するには、次のコマンドのいずれかを入力します。

- **zone** *new-zone-name* [*template-name*] [**interactive**]：Guard モジュールは新しいゾーンを作成します。*template-name* 引数を挿入しない場合、新しいゾーンは GUARD_DEFAULT ゾーン テンプレートから作成されます。
- **zone** *zone-name* [*template-name*] [**interactive**]：Guard モジュールは、既存のゾーンを削除し、同じ名前で新しいゾーンを作成します。

システム定義のゾーン テンプレートを使用する場合、Guard モジュールはゾーンのアトリビュートすべてにデフォルト設定を適用します。これらのデフォルト ポリシーの設定は、オンデマンド保護用に調整されます。

コマンドが正常に実行されると、Guard モジュールは新しいゾーンの設定モードに入ります。

ゾーン テンプレートを指定しないで既存のゾーンの名前を入力すると、Guard モジュールは指定されたゾーンの設定モードに入ります。

表 6-1 に、**zone** コマンドの引数とキーワードを示します。

表 6-1　zone コマンドの引数とキーワード

パラメータ	説明
new-zone-name	新しいゾーンの名前。名前は、1 ～ 63 文字の英数字の文字列です。この文字列は英字で始まる必要があり、アンダースコアを含むことができますが、スペースを含むことはできません。
zone-name	既存のゾーンの名前。
template-name	（オプション）ゾーンの設定を定義するゾーン テンプレート。デフォルトでは、GUARD_DEFAULT ゾーン テンプレートを使用してゾーンが作成されます。 詳細については、表 6-2 を参照してください。

表 6-1　zone コマンドの引数とキーワード（続き）

パラメータ	説明
interactive	Guard モジュールがゾーン保護をインタラクティブに実行するように設定します。ポリシーが作成する動的フィルタは、推奨事項として表示されます。各動的フィルタをアクティブにするかどうかを決定する必要があります。詳細については、第 9 章「インタラクティブ保護モード」を参照してください。

表 6-2 に、ゾーン テンプレートを示します。

表 6-2　ゾーン テンプレート

テンプレート	説明
GUARD_DEFAULT	デフォルトのゾーン テンプレート。Guard モジュールは、パケットの送信元 IP アドレスを Guard モジュールの TCP プロキシ IP アドレスに変更する場合があります。このゾーン テンプレートは、該当のゾーン ネットワークの着信 IP アドレスに基づく IP ベースのアクセス リスト（ACL）、アクセス ポリシー、またはロード バランシング ポリシーを使用しない場合に使用することができます。
GUARD_TCP_NO_PROXY	TCP プロキシを使用しないゾーン用に設計されたゾーン テンプレート。このゾーン テンプレートは、ゾーンが IP アドレスに従って管理される場合（Internet Relay Chat（IRC; インターネット リレー チャット）サーバ タイプのゾーンなど）や、ゾーンで実行されているサービスのタイプが不明な場合に使用することができます。

表 6-2　ゾーン テンプレート（続き）

テンプレート	説明
帯域幅限定リンク テンプレート	帯域幅のわかっているゾーンに応じてセグメント化された大規模なサブネットのオンデマンド保護用に設計されたゾーン テンプレート。これらのゾーンについては、**activation-extent ip-address-only** コマンドを使用して、攻撃されているサブネットまたは範囲に基づいてゾーン保護をアクティブにすることをお勧めします。このようなゾーンは、protect-ip-state が dst-ip-by-name となっている Detector で定義することを推奨します。 ポリシーのしきい値は、ゾーンへのトラフィックのレートが指定のレートを超過した場合に Guard モジュールがゾーンに対する攻撃を識別するように調整されます。 帯域幅限定リンク ゾーン テンプレートは、128 Kb、1 Mb、4 Mb、および 512 Kb のリンクをそれぞれ対象とした次のものが用意されています。 **GUARD_LINK_128K** **GUARD_LINK_1M** **GUARD_LINK_4M** **GUARD_LINK_512K** これらのテンプレートから作成されたゾーンに対してポリシー構築を実行することはできません。

次の例は、新しいゾーンを作成する方法を示しています。

```
user@GUARD-conf# zone scannet interactive
user@GUARD-conf-zone-scannet#
```

ゾーンを削除するには、**no zone** コマンドを使用します。ゾーンを削除するときは、ゾーン名の末尾に、ワイルドカード文字としてアスタリスク（*）を使用できます。ワイルドカードを使用すると、同じプレフィクスを持つ複数のゾーンを 1 つのコマンドで削除できます。

ゾーン テンプレートを表示するには、グローバル モードまたは設定モードで **show templates** コマンドを使用します。ゾーン テンプレートのデフォルト ポリシーを表示するには、グローバル モードまたは設定モードで **show templates** *template-name* **policies** コマンドを使用します。

ゾーンの複製

既存のゾーンに基づいて、新しいゾーンを作成することができます。既存のゾーンを新しいゾーンのテンプレートとして使用すると、既存のゾーンのプロパティすべてが、新しく定義したゾーンにコピーされます。スナップショットを指定すると、ゾーン ポリシーはスナップショットからコピーされます。

ゾーンを複製するには、次のコマンドのいずれかを入力します。

- **zone** *new-zone-name* **copy-from-this** [*snapshot-id*]：このコマンドは、現在のゾーンの設定を使用して新しいゾーンを作成するときに、ゾーン設定モードで使用します。
- **zone** *new-zone-name* **copy-from** *zone-name* [*snapshot-id*]：このコマンドは、特定のゾーンの設定を使用して新しいゾーンを作成するときに、設定モードで使用します。

表 6-3 で、**zone** コマンドの引数について説明します。

表 6-3　zone コマンドの引数

パラメータ	説明
new-zone-name	新しいゾーンの名前。名前は、1 ～ 63 文字の英数字の文字列です。この文字列は英字で始まる必要があり、アンダースコアを含むことができますが、スペースを含むことはできません。
zone-name	既存のゾーンの名前。
snapshot-id	既存のスナップショットの ID。詳細については、P.8-42 の「スナップショットの表示」を参照してください。

次の例は、現在のゾーンに関連して新しいゾーンを作成する方法を示しています。

```
user@GUARD-conf-zone-scannet# zone mailserver copy-from-this
user@GUARD-conf-zone-mailserver#
```

コマンドが正常に実行されると、Guard モジュールは新しいゾーンの設定モードに入ります。

新しいゾーンのポリシーには、未調整のマークが付けられます。ラーニング プロセスのしきい値調整フェーズを実行して、ポリシーのしきい値をゾーンのトラフィックに合せて調整する方法をお勧めします。新しいゾーンのトラフィック特性が、元になるゾーンのトラフィック特性と同じか、よく似ていれば、ポリシーのしきい値に調整済みのマークを付けることができます。詳細については、P.6-27 の「ポリシーへの調整済みのマーク付け」を参照してください。

新しいゾーンのアクティベーション インターフェイスは、ソース ゾーンの設定に関係なく zone-name-only に設定されます。詳細については、P.6-39 の「アクティベーション方式の設定」を参照してください。

ゾーンのアトリビュートの設定

ゾーンを作成したら、ゾーンのアトリビュートを設定できます。

ゾーンのアトリビュートを設定するには、次の手順を実行します。

ステップ 1　ゾーン設定モードに入ります。すでにゾーン設定モードになっている場合、このステップは省略してください。

ゾーン設定モードに入るには、次のコマンドのいずれかを入力します。

- **conf** *zone-name*：グローバル モードから
- **zone** *zone-name*：設定モードまたはゾーン設定モードから

zone-name 引数には、既存のゾーンの名前を指定します。

ステップ 2　ゾーンの IP アドレスを定義します。Guard モジュールがゾーン トラフィックをラーニングし、ゾーンを保護することを可能にするには、IP アドレスを定義する必要があります。

ゾーンの IP アドレスを設定するには、次のコマンドを入力します。

```
ip address ip-addr [ip-mask]
```

表 6-4 に、**ip address** コマンドの引数を示します。

表 6-4　ip address コマンドの引数

パラメータ	説明
ip-addr	ゾーンの IP アドレス。ゾーンは、サブネットでもかまいません。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
ip-mask	（オプション）IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。

ゾーン保護をアクティブにするには、IP アドレスを少なくとも 1 つ定義する必要があります。ゾーンの IP アドレスおよびサブセットはいつでも追加できます。

ゾーンの IP アドレスまたはサブセットを変更する場合は、次のタスクのいずれかを実行します。

- 新しい　IP　アドレスまたはサブネットが新しいサービスで構成され、そのサービスがゾーンのネットワークで定義されたことがない場合は、ゾーン保護をアクティブにする前にポリシー構築フェーズをアクティブにするか、サービスを手動で追加します。詳細については、P.6-17 の「ポリシーの構築」および P.8-15 の「サービスの追加」を参照してください。
- ゾーンが保護およびラーニング状態にある場合は、**no learning-params threshold-tuned** コマンドを使用して、ゾーン ポリシーに未調整のマークを付けます。ゾーンに対する攻撃がある場合は、ゾーン ポリシーのステータスを未調整に変更しないでください。これは、ステータスを変更すると Guard モジュールで攻撃が検出されなくなり、Guard モジュールが悪意のあるトラフィックのしきい値をラーニングするためです。詳細については、P.6-27 の「ポリシーへの調整済みのマーク付け」を参照してください。
- ゾーンが保護およびラーニングの動作状態になく、保護およびラーニングの動作状態をアクティブにする予定がない場合は、しきい値調整フェーズをアクティブにしてから、ゾーン保護をアクティブにします。P.6-19 の「しきい値の調整」を参照してください。

ステップ 3　（オプション）ゾーンで処理可能と考えられるトラフィックのレートに応じて、Guard モジュールがゾーンに再び注入するトラフィックの帯域幅を制限します。

次のコマンドを入力します。

rate-limit {**no-limit** | *rate burst-size rate-units*}

帯域幅の値は、ゾーンへの送信で測定された最大の帯域幅に設定することをお勧めします。この値が不明な場合は、デフォルトの帯域幅の値（無制限）のままにします。

表 6-5 に、**rate limit** コマンドの引数を示します。

表 6-5　rate limit コマンドの引数

パラメータ	説明
no-limit	ゾーンが無制限のレート リミットで定義されるよう指定します。
rate	ゾーンに通すことのできるトラフィック量を指定する、64 より大きな整数。単位は、*rate-units* 引数で指定されます。*レート* リミットは、最大で*バースト* リミットの 10 倍まで指定可能です。
burst	ゾーンに通すことのできるトラフィックの最大ピーク量を指定する、64 より大きな整数。単位は、*rate-units* 引数で指定されるレートの単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。*バースト* リミットは、最大で *レート* リミットの 8 倍まで指定可能です。
rate-units	レートの単位。次の単位があります。 • **bps**：ビット / 秒 • **kbps**：キロビット / 秒 • **kpps**：キロパケット / 秒 • **mbps**：メガビット / 秒 • **pps**：パケット / 秒

ステップ 4　（オプション）識別の目的で、ゾーンの説明を追加します。次のコマンドを入力します。

```
description string
```

文字列の長さは最大 80 文字です。

ゾーンの説明を変更するには、ゾーンの説明を再入力します。前の説明は新しい説明で上書きされます。

ステップ 5　新しく設定されたゾーンの設定を表示します。ゾーン設定モードで **show running-config** コマンドを使用します。

設定情報は、Guard モジュールを現在の設定値で設定するために実行される CLI コマンドで構成されています。詳細については、特定のコマンド エントリを参照してください。

次の例は、新しいゾーンを作成し、ゾーンのアトリビュートを設定する方法を示しています。

```
user@GUARD-conf# zone scannet
user@GUARD-conf-zone-scannet# ip address 192.168.100.34 255.255.255.252
user@GUARD-conf-zone-scannet# rate-limit 1000 2300 pps
user@GUARD-conf-zone-scannet# description Demonstration zone
```

ゾーン トラフィックの特性のラーニング

この項では、Guard モジュールのラーニング プロセスを使用してゾーンのトラフィック特性を分析し、Guard がゾーン保護に使用するポリシーを作成および微調整する方法について説明します。

この項では、次のトピックについて取り上げます。

- ラーニング プロセスの概要
- ゾーンのラーニング プロセスの結果と Cisco Traffic Anomaly Detector Module の同期
- ポリシーの構築
- しきい値の調整
- ラーニング パラメータの設定

ラーニング プロセスの概要

ラーニング プロセスでは、Guard が通常のゾーン トラフィックの特性をラーニングします。Guard モジュールはラーニング プロセスの結果を使用して、ゾーン保護のポリシーを作成します。これらのポリシーは、ゾーンのトラフィック フローの処理方法を Guard に指示します。

ポリシーを構築する最初のラーニング プロセスが終了したら、ラーニング プロセスとゾーン保護を同時にアクティブにできます。同時に、Guard モジュールはポリシーのしきい値を調整し、トラフィックの異常に関するポリシーのしきい値を監視します。このプロセスでは、Guard モジュールはゾーンを保護し、同時にゾーンのトラフィック特性に応じてポリシーのしきい値を常に更新することができます。また、Guard モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。

ゾーンのトラフィック特性をラーニングするには、ゾーンのトラフィックを Guard に宛先変更する必要があります。外部デバイスを使用して、ラーニング プロセスを開始する前に宛先変更を設定するか、ゾーンのトラフィックを Guard に手動で宛先変更する必要があります。Guard のルーティング設定を使用して、ゾーンの宛先変更を設定してください。

詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

ラーニング プロセスは、次の 2 つのフェーズで構成されます。

1. ポリシー構築：Guard はポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービスを検出できます。既存のポリシーが新しいポリシーで上書きされます。

   ポリシー テンプレートは、Guard のポリシー構築用ツールです。このテンプレートは、Guard が作成するゾーン ポリシーのタイプを定義します。また、ポリシー テンプレートは、Guard が厳密に監視するサービスの最大数と、Guard による新しいポリシーの作成をトリガーする最小しきい値も定義します。ゾーン ポリシーを構築するための指針となる規則を変更するには、ポリシー テンプレート パラメータを変更してから、ポリシー構築フェーズを開始します。詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください。

2. しきい値の調整：Guard はゾーンのサービスのトラフィック レートに合せてポリシーを調整します。トラフィックが透過的に Guard を通過し、Guard はゾーン ポリシーの構築中に検出されたサービスのしきい値を調整できます。既存のしきい値が新しいしきい値で上書きされます。

   しきい値調整フェーズとゾーン保護を同時にアクティブにすると（保護およびラーニング モード）、Guard モジュールで悪意のあるトラフィックのしきい値がラーニングされなくなります。Guard が常にポリシーを調整するように設定し、Guard がポリシーのしきい値を更新するときの間隔を定義することができます。

（注） 保護およびラーニング モードにおいて Guard モジュールをアクティブにすると、ゾーン トラフィックは常に Guard モジュールに宛先変更されます。

Guard は、ゾーンのトラフィックの特性をラーニングして、ゾーンのトラフィックを比較する基準とし、悪意の攻撃となる可能性のあるあらゆる異常をトレースします。Guard は、ラーニング プロセス中は、現在のゾーン ポリシーを変更しません。Guard がポリシーを更新するのは、ラーニング フェーズのいずれかの段階における結果を受け入れるように指定した場合のみです。

ポリシーが作成された後は、ポリシーを追加または削除できます。また、しきい値、サービス、タイムアウト、アクションなどのポリシー パラメータを変更することもできます。

snapshot threshold-selection cur-thresholds コマンドを使用すると、現在のゾーン ポリシーをいつでもバックアップできます。詳細については、P.8-38 の「スナップショットの作成」を参照してください。

（注） ラーニング プロセスでは、Guard がパケットをドロップするのは、パケットにある送信元 IP アドレス、プロトコル番号、UDP 送信元または宛先ポート、および TCP 送信元または宛先ポートの各フィールドのいずれかがゼロの場合だけです。

ラーニング プロセスが完了する前にゾーンに対する攻撃があった場合、次の条件のいずれかに該当するときは、オンデマンド保護を使用してゾーンを保護します。

- ゾーンがラーニング プロセスの実行中である。
- Guard モジュールが保護およびラーニング モードになっているが、ゾーンのトラフィック特性をラーニングしていない。
- ゾーンのトラフィックを表さないと考えられるポリシーのしきい値を受け入れている。

詳細については、P.6-45 の「オンデマンド保護のイネーブル化」を参照してください。

複数のゾーンに対して同時に**ラーニング**関連のコマンドを発行できます。これには、グローバル モードで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてポリシー構築フェーズを開始する場合は、グローバル モードで **learning policy-construction * コマンド**を入力します。*scan* で始まる名前を持つ Guard モジュールのすべてのゾーン（scannet や scanserver など）のポリシー構築フェーズの結果を受け入れるには、グローバル モードで **no learning** *scan**** **accept** コマンドを入力します。

ゾーンのラーニング プロセスの結果と Cisco Traffic Anomaly Detector Module の同期

Cisco Traffic Anomaly Detector Module（Detector モジュール）が常にゾーン トラフィックをラーニングし、Guard のゾーン ポリシーを更新するように設定できます。

Detector モジュールはゾーンに対する攻撃を検出すると、ラーニング プロセスを停止し、Guard モジュールによるゾーン保護をアクティブにします。攻撃が終了すると、ゾーン トラフィックのラーニングを再開します。このプロセスでは、ゾーン ポリシーのしきい値を継続的に調整する一方で、ゾーン トラフィックを常に Guard モジュールに宛先変更することを回避できます。

ラーニング プロセスの結果を Detector モジュールに同期させるには、次のタスクを実行する必要があります。

1. Guard モジュールを Detector モジュールのリモート Guard SSL リストのいずれかに追加します。
2. Detector モジュールと SSL 通信チャネルを確立します（P.4-24 の「SSL 通信チャネルの設定」を参照）。
3. GUARD ゾーン テンプレートを使用して、Detector モジュール上にゾーンを作成します。

ゾーン設定を Detector モジュールに同期させることや、ゾーン設定を Detector モジュールに自動的に同期させるように Detector モジュールを設定することが可能です。詳細については、P.6-30 の「Guard モジュールのゾーン設定と Detector モジュールの同期」を参照してください。

このオプションは、Detector モジュールだけで設定できます。詳細については、『*Cisco Trafiic Anomaly Detector Module Configuration Guide*』を参照してください。

ポリシーの構築

ポリシー構築フェーズでは、Guard はポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービス（ポートとプロトコル）を検出できます。ポリシー構築の指針となる規則を設定することもできます。たとえば、Guard で特定のタイプのポリシーが作成されないようにするには、関連するポリシー テンプレートをディセーブルにします。ゾーン ポリシーを構築するための規則を変更するには、ポリシー テンプレート パラメータを変更してから、ポリシー構築フェーズを開始します。詳細については、P.8-5 の「ポリシー テンプレートについて」を参照してください。

Guard は、ポリシー パラメータ（タイムアウト、アクション、およびしきい値）のデフォルト値を設定します。動作パラメータのデフォルト値の設定方法については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください。

このフェーズで Guard が作成する新しいポリシーは、既存のポリシーを上書きします。

（注） 帯域幅限定リンク ゾーン テンプレート（GUARD_LINK_128K、GUARD_LINK_1M、GUARD_LINK_4M、および GUARD_LINK_512K）に基づくゾーンに対しては、ポリシー構築を実行できません。

ゾーン ポリシーを構築するには、次の手順を実行します。

ステップ 1　ポリシー構築フェーズを開始します。ゾーン設定モードで次のコマンドを入力します。

```
learning policy-construction
```

ヒント　Guard　モジュールがゾーンのトラフィックの宛先変更を実行していることを確認してください。ポリシー構築またはしきい値調整を開始してから少なくとも 10 秒待ってから、**show rates details** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、宛先変更に問題があることを示しています。

ステップ 2　（オプション）Guard モジュールが構築しているポリシーを表示します。ポリシー構築フェーズの任意の段階でラーニング パラメータ（サービス、しきい値、およびポリシー関連のその他のデータ）のスナップショットを保存しておいて、後で確認することができます。単一のスナップショットを保存するか、定期的なスナップショットを（指定した間隔で）保存することができます。詳細については、P.8-38 の「スナップショットを使用したラーニング プロセスの結果の確認」を参照してください。

ステップ 3　（オプション）ポリシー構築フェーズを長期間実行する場合、ポリシー構築フェーズを停止しなくても、Guard によって提案されたポリシーを受け入れることができます。ポリシーを 1 回受け入れるか、提案されたポリシーを Guard が指定された間隔で自動的に受け入れるように定義できます。このようにすると、ゾーンが最新のポリシーを持つと同時に、継続してゾーンのトラフィックをラーニングすることを保証できます。

Guard によって提案されたポリシーを受け入れ、ポリシー構築フェーズを継続するには、次のコマンドを入力します。

```
learning accept
```

Guard によって提案されたポリシーを指定した間隔で自動的に受け入れるには、次のコマンドを入力します。

```
learning-params periodic-action auto-accept learn_params_days
learn_params_hours learn_params_minutes
```

詳細については、P.6-24 の「ラーニング パラメータの設定」を参照してください。

定期的なアクションを終了するには、**no learning-params periodic-action** コマンドを使用します。

ステップ 4　十分に時間をおいてからポリシー構築フェーズを終了し、新しく構築されたポリシーの取り扱いを決定します。

ポリシー構築フェーズを終了する前に、少なくとも 2 時間はこのフェーズを続けることを推奨します。

次のいずれかを行うことができます。

- **提案されたポリシーの受け入れ：**Guard によって提案されたポリシーを受け入れるには、ゾーン設定モードで次のコマンドを入力します。

  no learning accept

  Guard は、以前にラーニングしたポリシーとしきい値を消去します。

  新しく構築されたポリシーを受け入れた後は、手動でポリシーを追加または削除できます。詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- **提案されたポリシーの拒否：**Guard によって提案されたポリシーを拒否するには、ゾーン設定モードで次のコマンドを入力します。

  no learning reject

  Guard はプロセスを停止し、ラーニングした新しいポリシーを保存しません。ゾーンのポリシーは、ラーニング プロセスを開始する前のままになるか、ポリシー構築フェーズの結果を最後に受け入れる前のままになります。

次の例は、ポリシー構築フェーズを開始し、提案されたポリシーを 12 時間間隔で受け入れる方法を示しています。例では、次に、ポリシー構築フェーズを停止し、提案されたポリシーを受け入れます。

```
user@GUARD-conf-zone-scannet# learning policy-construction
user@GUARD-conf-zone-scannet# learning-params periodic-action auto-accept 0 12 0
user@GUARD-conf-zone-scannet# no learning accept
```

しきい値の調整

しきい値調整フェーズでは、Guard がゾーンのトラフィックを分析し、ポリシー構築フェーズで構築されたポリシーのしきい値を定義します。

ゾーンのトラフィックをラーニングし、同時にトラフィックの異常に関するポリシーの、最後に受け入れられたしきい値を監視するように、Guard モジュールを設定できます。Guard モジュールはゾーンに対する攻撃を検出すると、しきい値調整フェーズを停止しますが、ゾーン保護は継続します。この結果、Guard モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。

攻撃が終了すると、Guard モジュールはラーニング プロセスを再開します。攻撃が終了してからラーニング プロセスを再度アクティブにするまで、Guard モジュールは、protection-end-timer で定義された期間（最大で 10 分）待機します。詳細については、P.6-43 の「保護の無活動タイムアウトの設定」を参照してください。

（注） しきい値調整フェーズは、トラフィックのピーク時（最も忙しい日）に、少なくとも 24 時間実行することを推奨します。

ポリシーのしきい値を調整するには、次の手順を実行します。

ステップ 1　しきい値調整フェーズを開始します。

保護およびラーニング モードを開始すること、つまり、しきい値調整フェーズをアクティブにすると同時に Guard がゾーンを保護するように設定することをお勧めします。ゾーン設定モードで次のコマンドを入力します。

```
protect learning
```

または、learning threshold-tuning コマンドと protect コマンドを順番に発行します（順序は問いません）。

ヒント　Guard　モジュールがゾーンのトラフィックの宛先変更を実行していることを確認してください。ポリシー構築またはしきい値調整を開始してから少なくとも 10 秒待ってから、**show rates details** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、宛先変更に問題があることを示しています。

Guard モジュールはゾーンに対する攻撃を検出すると、しきい値調整フェーズを停止しますが、ゾーン保護は継続します。

（注）　ゾーンへのトラフィックが穏やかなときに保護およびラーニング モードを開始すると、Guard モジュールは、ピーク時のトラフィックを攻撃と見なす場合があります。このような場合は、次のいずれかを行うことができます。

- ポリシーのしきい値の状態を未調整に設定する。ゾーン設定モードで **learning-params threshold-tuned** コマンドを使用します。詳細については、P.6-27 の「ポリシーへの調整済みのマーク付け」を参照してください。
- ゾーン保護を非アクティブにし、継続してポリシーのしきい値をラーニングする。ゾーン設定モードで **no protect** コマンドを使用します。

ゾーン保護としきい値調整フェーズを同時に非アクティブにするには、ゾーン設定モードで **deactivate** コマンドを使用します。

しきい値調整フェーズだけをアクティブにするには、learning threshold-tuning コマンドを使用します。

ステップ 2　（オプション）Guard モジュールが調整しているポリシーを表示します。しきい値調整フェーズの任意の段階で、ラーニング パラメータ（サービス、しきい値、およびポリシー関連のその他のデータ）のスナップショットを保存できます。後でスナップショットを確認することや、ラーニング パラメータを別のスナップショットと比較することができます。単一のスナップショットを保存するか、定期的なスナップショットを（指定した間隔で）保存することができます。詳細については、P.8-38 の「スナップショットを使用したラーニング プロセスの結果の確認」を参照してください。

ステップ 3　Guard によって提案されたポリシーを受け入れ、しきい値調整フェーズを継続することができます。ポリシーを 1 回受け入れるか、提案されたポリシーを Guard が指定された間隔で自動的に受け入れるように定義できます。このようにすると、ゾーンが最新のポリシーを持つと同時に、継続してゾーンのトラフィックをラーニングすることを保証できます。

Guard によって提案されたポリシーを受け入れ、しきい値調整フェーズを継続するには、次のコマンドを入力します。

```
learning accept [threshold-selection {new-thresholds | max-thresholds
| weighted weight}]
```

threshold-selection の引数とキーワードについては、表 6-7 を参照してください。

Guard によって提案されたポリシーを指定した間隔で自動的に受け入れるには、次のコマンドを入力します。

```
learning-params periodic-action auto-accept learn_params_days
learn_params_hours learn_params_minutes
```

詳細については、P.6-24 の「ラーニング パラメータの設定」を参照してください。

定期的なアクションを終了するには、**no learning-params periodic-action** コマンドを使用します。

ステップ 4　十分な時間が経過してから、しきい値調整フェーズを終了し、新しく調整されたポリシーの処理方法を決定します。

ただし、Guard モジュールが常にゾーン トラフィックを宛先変更している場合は、ゾーンを保護およびラーニング モードのままにし、しきい値調整フェーズを終了しないことをお勧めします。

次のアクションのいずれかを行うことができます。

- **提案されたポリシーの受け入れ：**Guard によって提案されたポリシーのしきい値を受け入れるには、ゾーン設定モードで次のコマンドを入力します。

  ```
  no learning accept [threshold-selection {new-thresholds |
  max-thresholds | weighted weight}]
  ```

  threshold-selection の引数とキーワードについては、表 6-7 を参照してください。

  Guard は、以前にラーニングしたしきい値を消去します。

  新しく調整されたポリシーを受け入れた後は、手動でポリシーのパラメータを変更することができます。詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- **提案されたポリシーの拒否**：Guard によって提案されたポリシーのしきい値を拒否するには、ゾーン設定モードで次のコマンドを入力します。

  ```
  no learning reject
  ```

この場合、Guard はしきい値調整フェーズを停止し、しきい値調整フェーズを開始する前のしきい値の状態に戻ります。その結果、新しく構築されたポリシーには、以前のトラフィック特性に基づいて取得したしきい値が使用される場合があります。

次の例は、しきい値調整フェーズを開始し、提案されたポリシーを 1 時間間隔で受け入れる方法を示しています。例では、次に、しきい値調整フェーズを停止し、しきい値が現在の値よりも大きい場合に、提案されたポリシーを受け入れます（*max-thresholds* 方式）。

```
user@GUARD-conf-zone-scannet# learning threshold-tuning
user@GUARD-conf-zone-scannet# learning-params periodic-action
auto-accept 0 1 0
user@GUARD-conf-zone-scannet# no learning accept threshold-selection
max-thresholds
```

ラーニングの結果を表示するには、**show policies statistics** コマンドを使用します。

詳細については、P.8-34 の「ポリシーの表示」を参照してください。

ラーニングしたしきい値を確認した後は、結果の一部を変更できます。この変更がその後のしきい値調整フェーズで上書きされないようにするには、次のアクションのいずれかを実行します。

- ポリシーのしきい値を固定値として設定する：Guard は新しいしきい値を無視し、現在のしきい値を保持します。詳細については、P.8-25 の「固定値としてのしきい値の設定」を参照してください。
- ポリシーの固定乗数を設定する：新しいポリシーのしきい値を計算する場合は、ラーニングしたしきい値に指定の乗数を掛け、その結果にしきい値選択方式を適用します。詳細については、P.8-26 の「しきい値の乗数の設定」を参照してください。

ラーニング パラメータの設定

ラーニング パラメータを使用すると、Guard モジュールが実行できるラーニング関連のアクションと、Guard モジュールが指定のポリシーを処理する方法を設定できます。次のパラメータを定義できます。

- **periodic-action**：ポリシーのスナップショットを保存し、ポリシーを自動的に受け入れるように Guard モジュールを設定できます。または、ポリシーのスナップショットを指定された間隔だけで保存するように Guard モジュールを設定できます。P.6-25 の「定期的なアクションの設定」を参照してください。
- **threshold-tuned**：ゾーンのポリシーに調整済みのマークを付けます。ゾーンのポリシーに調整済みのマークが付いていない場合、Guard モジュールはゾーンに対する攻撃を検出しません。P.6-27 の「ポリシーへの調整済みのマーク付け」を参照してください。
- **threshold-selection**：しきい値調整フェーズの結果を受け入れた場合に、新しいポリシーのしきい値を生成するために Guard モジュールが使用するデフォルトの方式を設定します。P.6-26 の「しきい値選択方式の設定」を参照してください。
- **fixed-threshold**：ポリシーのしきい値を固定値として設定します。Guard モジュールは、以後のしきい値調整フェーズにおいてポリシーのしきい値を変更しません。P.8-25 の「固定値としてのしきい値の設定」を参照してください。
- **threshold-multiplier**：ポリシーのしきい値の固定乗数を設定します。Guard モジュールは、以後のしきい値調整フェーズでは、現在のポリシーのしきい値、ラーニングされたしきい値、および固定乗数に基づいて、ポリシーのしきい値を計算します。P.8-26 の「しきい値の乗数の設定」を参照してください。

ラーニング パラメータの設定を表示するには、ゾーン設定モードで **show learning-params** コマンドを使用します。

定期的なアクションの設定

ポリシーのスナップショットを保存し、ポリシーを自動的に受け入れるように Guard モジュールを設定できます。または、ポリシーのスナップショットを指定された間隔だけで保存するように Guard モジュールを設定できます。スナップショットの詳細については、P.8-34 の「ポリシーの監視」を参照してください。

定期的なアクションを設定するには、次のコマンドを入力します。

learning-params periodic-action {**auto-accept** | **snapshot-only**}
learn_params_days learn_params_hours learn_params_minutes

表 6-6 で、**learning-params** コマンドの引数とキーワードについて説明します。

表 6-6　learning-params periodic-action コマンドの引数とキーワード

パラメータ	説明
auto-accept	Guard によって提案されたポリシーを、指定された間隔で受け入れます。Guard は新しく提案されたゾーン ポリシーを受け入れた後で、ゾーン ポリシーのスナップショットを保存します。
snapshot-only	指定された間隔でポリシーのスナップショットを保存します。Guard は新しいポリシーを受け入れず、ポリシーのしきい値を変更しません。
learn_params_days	間隔（日単位）。0 ～ 1000 の整数を入力します。
learn_params_hours	間隔（時間単位）。0 ～ 1000 の整数を入力します。
learn_params_minutes	間隔（分単位）。0 ～ 1000 の整数を入力します。

間隔の値は、*learn_params_days*、*learn_params_hours*、および *learn_params_minutes* の合計となります。

次の例は、ポリシーを 1 時間間隔で受け入れるように Guard モジュールを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# learning-params periodic-action auto-accept 0 1 0
```

しきい値選択方式の設定

しきい値調整フェーズで新しいポリシーのしきい値が受け入れられた場合に、新しいしきい値を生成するために Guard モジュールが使用するデフォルトの方式を設定できます。しきい値調整フェーズの結果を手動で受け入れること、またはしきい値調整フェーズの結果を指定された間隔で自動的に受け入れるように Guard モジュールを設定することが可能です。

次のコマンドを入力します。

learning-params threshold-selection {**new-thresholds** | **max-thresholds** | **weighted weight**}

表 6-7 で、**learning-params threshold-selection** コマンドの引数とキーワードについて説明します。

表 6-7　learning-params threshold-selection コマンドの引数とキーワード

パラメータ	説明
new-thresholds	Guard モジュールは、ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	Guard モジュールは、ポリシーの現在のしきい値とラーニング済みのしきい値とを比較し、2 つのうちで大きな方の値をゾーン設定に保存します。 これがデフォルトの方法です。
weighted *weight*	Guard モジュールは、保存するポリシーしきい値を次の式に基づいて計算します。 新しいしきい値 =（ラーニングしたしきい値 * 重み + 現在のしきい値 *（100 - 重み））/ 100

次の例は、ラーニングされたしきい値が現在のポリシーのしきい値よりも大きい場合に、提案されたポリシーを受け入れるように Guard モジュールを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# learning-params threshold-selection max-thresholds
```

ポリシーへの調整済みのマーク付け

Guard モジュールは、ポリシーのしきい値のステータス（ポリシーのしきい値が調整済みかどうかということ）にマークを付けます。保護およびラーニング モードのときは、このステータスに関連付けられます。ポリシーのしきい値のステータスは、ポリシーのしきい値超過が発生したときに Guard モジュールがゾーンに対する攻撃を識別するかどうかを示します。

新しいゾーンが作成された場合、またはゾーンのポリシー構築フェーズの結果が受け入れられた場合、Guard モジュールはゾーン ポリシーのしきい値に未調整のマークを付けます。ゾーン テンプレートのデフォルトのしきい値は、Guard モジュールがゾーンのトラフィックに異常を発見した場合にスプーフィング防止メカニズムをすぐにアクティブにするように調整されています。そのため、Guard モジュールが保護およびラーニング モードの場合は、ラーニング プロセスが停止することがあります。このような状況を避けるため、Guard モジュールは、保護およびラーニング モードでゾーン ポリシーが調整済みでない場合は（ゾーン ポリシーのしきい値が一度受け入れられるまでは）、ゾーン トラフィックの攻撃を検出しません。

ゾーン ポリシーが未調整の場合、Guard モジュールは accept-new のしきい値選択方式だけをアクティブにします（P.6-26 の「しきい値選択方式の設定」を参照）。Guard モジュールは、以前のしきい値を無視して、新しいしきい値を受け入れます。これは、そのゾーンに関するラーニング プロセスのしきい値調整フェーズの結果を受け入れるときに、accept-new 以外のしきい値選択方式を使用すると、ポリシーのしきい値の集合が不適切になる場合があるためです。

次の場合、Guard モジュールは、ゾーン ポリシーに未調整のマークを付けます。

- 新しいゾーンを作成する場合
- ポリシー構築フェーズの結果を受け入れた場合
- ゾーン ポリシーに対してサービスの削除または新しいサービスの追加を行った場合

しきい値調整フェーズの結果を受け入れると、Guard モジュールは、ゾーン ポリシーに調整済みのマークを付けます。

ユーザは、ゾーン ポリシーの設定を変更できます。ゾーン ポリシーに調整済みのマークを付けるには、ゾーン設定モードで次のコマンドを入力します。

learning-params threshold-tuned

ゾーン ポリシーに未調整のマークを付けるには、このコマンドの **no** 形を使用します。

次のどちらかの場合は、ゾーン ポリシーのステータスを調整済みに変更してもかまいません。

- 新しいゾーンが既存のゾーンまたはスナップショットから複製されており、両方のゾーンのトラフィック特性が似ている場合
- ポリシーのしきい値をすべて手動で設定した場合

次のいずれかの場合は、ゾーン ポリシーのステータスを未調整に変更してもかまいません。

- ゾーンのネットワークに重要な変更を加えた場合
- ゾーンの IP アドレスまたはサブネットを変更した場合
- トラフィックのピーク時に保護およびラーニング　モードを開始しなかった場合（Guard モジュールではピーク時のトラフィックが攻撃と見なされなくなる）

Guard モジュールは現在のポリシーのしきい値に関連付けられず、しきい値超過が発生してもゾーンに対する攻撃を検出しません。

（注） ゾーンに対する攻撃がある場合は、ゾーン　ポリシーのステータスを未調整に変更しないでください。これは、ステータスを変更すると Guard モジュールで攻撃が検出されなくなり、Guard モジュールが悪意のあるトラフィックのしきい値をラーニングするためです。

次の例は、ゾーン ポリシーのステータスに調整済みのマークを付ける方法を示しています。

```
user@GUARD-conf-zone-scannet# learning-params threshold-tuned
```

ゾーン ポリシーのしきい値の調整とゾーン保護のイネーブル化の同時実行

ポリシーを構築する最初のラーニング プロセスが終了したら、ラーニング プロセスをアクティブにし、同時にゾーン保護をイネーブルにすることができます。Guard モジュールはポリシーのしきい値を調整し、同時にトラフィックの異常に関するポリシーのしきい値を監視します。この状態では、Guard モジュールはゾーンを保護し、同時にゾーンのトラフィック特性に応じてポリシーのしきい値を常に更新することができます。また、Guard モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。

新しいゾーンを作成した場合や、ゾーン ポリシーに対してサービスの追加または削除を行った場合、またはゾーンのポリシー構築フェーズの結果を受け入れた場合、Guard モジュールはゾーン ポリシーのしきい値に未調整のマークを付けます。ラーニング プロセスのしきい値調整フェーズの結果を受け入れた場合にのみ、Guard モジュールは、ゾーン ポリシーに調整済みのマークを付けます。

ラーニング プロセスとゾーン保護を同時にイネーブルにした場合、ゾーン ポリシーが調整済みでないときは、Guard モジュールは次のように動作します。

- Guard モジュールは、ゾーン トラフィックの攻撃を検出しません（ゾーン ポリシーのしきい値が一度受け入れられるまで）。
- Guard モジュールは、accept-new のしきい値選択方式だけをアクティブにします（P.6-26 の「しきい値選択方式の設定」を参照）。

Guard モジュールはゾーンに対する攻撃を識別すると、ラーニング プロセスを停止しますが、ゾーン保護は継続します。攻撃が終了すると、Guard モジュールは保護およびラーニング動作状態に戻ります。

ラーニング プロセスとゾーン保護を同時にアクティブにするには、**保護 learning** コマンドを使用するか、**learning threshold-tuning** コマンドと **保護**コマンドを順番に入力します（順序は問いません）。

詳細については、P.6-19 の「しきい値の調整」および P.6-35 の「ゾーンの保護」を参照してください。

Guard モジュールのゾーン設定と Detector モジュールの同期

ゾーンの設定とポリシーを Detector モジュール上のゾーンに同期させることができます。Detector モジュールは、完全なゾーン設定をコピーします。したがって、ゾーンを一度設定すれば、Guard モジュールと Detector モジュールの両方で同じ設定とポリシーを保持できます。

Detector モジュールと Guard モジュールの間の通信には、Secure Socket Layer（SSL）プロトコルが必要です。SSL には認証と暗号化が用意されています。ゾーンを同期させる前に、SSL 通信接続チャネルを設定する必要があります。詳細については、P.4-23 の「Cisco Traffic Anomaly Detector Module との通信のイネーブル化」を参照してください。

ゾーン ポリシーを最新の状態に保つためにゾーンのトラフィック特性を常にラーニングする一方で、ゾーン トラフィックを常に Guard モジュールに宛先変更することを回避するように、Detector モジュールを設定できます。

同期用のゾーンを作成し、Detector モジュールからゾーンを同期させる必要があります。詳細については、『*Cisco Trafiic Anomaly Detector Module Configuration Guide*』を参照してください。

この項では、次のトピックについて取り上げます。

- 設定のガイドライン
- サンプル シナリオ
- オフラインでのゾーン設定の同期

設定のガイドライン

Guard モジュールと Detector モジュールの間でゾーンを同期させる場合は、次のガイドラインを使用します。

- Guard モジュールと Detector モジュールの間でゾーンを同期させるには、Guard モジュールと Detector モジュールの両方に適したゾーン テンプレート（GUARD ゾーン テンプレート）を使用して、Detector モジュール上に新しいゾーンを作成する必要があります。

- ゾーン ポリシーが正しく同期されることを保証するには、Guard モジュール（トラフィックを宛先変更している場合）と Detector モジュールの両方に同じタイプのトラフィックが流れることを確認する必要があります。それ以外の場合は、ゾーンのグローバル ポリシーが高すぎるか、または低すぎるため、スプーフィングを利用した DDoS 攻撃から適切に保護されることを保証できません。
- Detector モジュールを集中設定ポイントとして使用します。Detector モジュールにゾーンを設定し、Detector モジュールの設定のバックアップを保持します。Detector モジュールから Guard モジュールにゾーン設定をコピーします。
- デバイスを物理的に変更した場合や、Detector モジュールと Guard モジュールが通信に使用するインターフェイスの IP アドレスを変更した場合は、Detector モジュールと Guard モジュールが安全な通信のために使用する SSL 証明書を再生成する必要があります。
- Guard モジュール上のゾーン設定を確認します。アクティベーション範囲が **ip-address-only** で、アクティベーション方式が **zone-name-only** 以外の場合は、**protection-end-timer** コマンドを使用して、ゾーンに対する攻撃が終了したことを識別するときに Guard モジュールが使用するタイマーを設定することをお勧めします。**protection-end-timer** の値が **forever** の場合、Guard モジュールは、ゾーンに対する攻撃が終了したことを識別せず、特定の IP アドレスを保護するために作成したサブゾーンを削除しません。

サンプル シナリオ

次の設定プロセスの例は、同期を使用して、現在のトラフィック特性に応じてゾーンが保護されることを保証する方法を示しています。

1. GUARD ゾーン テンプレートのいずれかを使用して、Detector モジュール上に新しいゾーンを作成および設定します。

   Guard モジュールでは、そのようなゾーンを識別するために、ゾーン設定モードでの **show** コマンド出力にあるゾーン ID フィールドの横に *(Guard/Detector)* が表示されます。

2. Guard モジュールを、Detector モジュール上にあるゾーンの SSL リモート Guard リストまたはデフォルトの SSL リモート Guard リストに追加します。
3. ゾーン ポリシーを構築するように Detector モジュールを設定します。**learning policy-construction** コマンドを使用します。

4. トラフィックの異常を検出しながら、ゾーン トラフィックをラーニングし、ポリシーのしきい値を調整するように Detector モジュールを設定します。**detect learning** コマンドを使用します。
5. ラーニングするポリシーのしきい値を 24 時間ごとに受け入れるように Detector モジュールを設定します。これにより、ゾーンのポリシーが、変化するトラフィック パターンで更新されることが保証されます。
6. ラーニングした新しいポリシーのしきい値を受け入れるたびに、ゾーン設定を Guard モジュールに同期させるように Detector モジュールを設定します。これにより、Detector モジュールがゾーン ポリシーをラーニングした場合に Guard モジュール上のゾーン ポリシーが更新されることが保証されます。
7. Guard モジュールによるゾーン保護をアクティブにする前に、ゾーン設定を Guard モジュール上の設定に同期させるように Detector モジュールを設定します。これにより、Guard モジュールがゾーンを保護する時点で Guard モジュール上のゾーンの設定とポリシーが最新の状態になっていることが保証されます。
8. Detector モジュールは、ゾーンに対する攻撃を検出すると、次のアクションを実行します。
   - Guard モジュール上のゾーン設定が最新の状態になっていることを確認する。Guard モジュール上のゾーン設定が Detector モジュール上のゾーン設定と異なる場合、Detector モジュールはゾーン設定を同期させます。
   - Guard モジュールによるゾーン保護をアクティブにする（Guard モジュールがゾーン保護をアクティブにします）。
   - ゾーンのラーニング プロセスを停止し、ゾーン トラフィックの異常の検出を継続する。この結果、Detector モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。

   攻撃が進行中でも、Guard 上でゾーンのポリシーを変更できます。

   Detector モジュールは常に Guard モジュールをポーリングします。攻撃が終了すると、Guard モジュールはゾーン保護を非アクティブにします。Detector モジュールは、Guard がゾーン保護を非アクティブにしたことを識別すると、ほかにトラフィック異常がないことを確認してから、検出およびラーニング動作状態を再度アクティブにします。
9. ゾーン ポリシーを攻撃の特性に合せて調整するように Guard モジュール上のゾーン ポリシーを手動で変更した場合は、新しいポリシーを Detector モジュールに再び同期させることができます。このことは、ゾーン トラフィックによって、特定のポリシーのしきい値を固定値として設定することや、ポリシーのしきい値の固定乗数を設定することが必要になった場合に重要に

なります。このようにすると、Detector モジュールが以後のしきい値調整フェーズでポリシーのしきい値に正しく関連し、Guard モジュールのポリシーが正しいしきい値で更新されることが保証されます。

詳細については、P.8-25 の「固定値としてのしきい値の設定」および P.8-26 の「しきい値の乗数の設定」を参照してください。

このアクションは、Detector モジュールだけで実行できます。詳細については、『*Cisco Trafiic Anomaly Detector Module Configuration Guide*』を参照してください。

オフラインでのゾーン設定の同期

Guard モジュールと Detector モジュールの間に安全な通信チャネルを確立できなくても、ゾーン設定を同期させることができます。次のいずれかの場合は、ゾーン設定をオフラインで同期させることが必要になる場合があります。

- Guard モジュールが Detector モジュールへのアクセス権を持っていない場合
- Detector モジュールが Guard モジュールへのアクセス権を持っていない場合
- Detector モジュールが Network Address Translation（NAT; ネットワーク アドレス変換）デバイスを介して Guard モジュールと通信する場合

ゾーン設定をオフラインで同期させるには、Detector モジュールから FTP またはセキュア FTP（SFTP）サーバにゾーン設定をエクスポートしてから、ゾーン設定を Guard モジュールに手動でインポートする必要があります。

Guard モジュールと Detector モジュールの間に安全な通信チャネルがないため、Detector モジュールがゾーン トラフィックの異常を検出するときは、Guard モジュールによるゾーン保護を手動でアクティブにする必要があります。

詳細については、P.6-35 の「ゾーンの保護」を参照してください。

Guard モジュールでのゾーン設定の同期をイネーブルにするには、GUARD ゾーン テンプレートのいずれかを使用して Detector モジュール上にゾーンを作成する必要があります。

ゾーンの設定をオフラインで同期させるには、次の手順を実行します。

ステップ 1　ゾーン設定をソース デバイスからエクスポートします。

copy zone *zone-name* **running-config ftp** コマンドを使用します。P.12-2 の「設定のエクスポート」を参照してください。

ステップ 2　ゾーンの設定を FTP または SFTP サーバからターゲット デバイスにインポートします。**copy ftp running-config** コマンドまたは **copy sftp running-config** コマンドを使用します。

ゾーン設定をインポートする前に、ゾーンを非アクティブにすることをお勧めします。詳細については、P.12-4 の「設定のインポートとアップデート」を参照してください。

ゾーンの保護

ゾーン保護をアクティブにする前に、Guard モジュールでゾーンのトラフィック パターンをラーニングすることをお勧めします。ラーニング プロセスにより、Guard モジュールで各ゾーンのトラフィック パターンをラーニングし、ゾーン トラフィックの統計分析に従って推奨のしきい値のセットを作成することができます。または、Cisco Traffic Anomaly Detector Module（Detector モジュール）から、ポリシーを含むゾーン設定を同期させることもできます。ゾーンの IP アドレス範囲が重なっていなければ、複数のゾーンを同時に保護できます。

ラーニング プロセスを開始する前に宛先変更を設定するか、ゾーンのトラフィックを Guard に手動で宛先変更する必要があります。Guard のルーティング設定を使用して、ゾーンの宛先変更を設定してください。

詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

ゾーンが攻撃を受けてなければ、保護およびラーニング モードにおいて Guard モジュールをアクティブにすることができます。Guard モジュールは、常にゾーン トラフィックを宛先変更し、ポリシーのしきい値を調整します。詳細については、P.6-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。

次の保護特性を定義できます。

- **動作モード**：Guard　モジュールがゾーンを自動的に保護する手段をとるか、インタラクティブに保護する手段をとるかを定義します。
- **アクティベーション方式**：ゾーンをアクティブにするときに、ゾーン名、ゾーンのアドレス範囲、または受信トラフィックのいずれに従うかを定義します。外部デバイス（Detector モジュールなど）によってゾーン保護をアクティブにする場合は、アクティベーション方式を設定する必要があります。
- **アクティベーション範囲**：ゾーン保護を、ゾーンのアドレス範囲全体についてアクティブにするか、ゾーン内の特定の IP アドレスに限定してアクティブにするかを定義します。アクティベーション範囲は、外部デバイスによってゾーン保護がアクティブにされたゾーンだけに適用されます。
- **保護の終了のタイムアウト**：Guard モジュールがゾーン保護を終了するまでのタイムアウトを定義します。

この項では、次のトピックについて取り上げます。

- ゾーン保護のアクティブ化
- ゾーン保護の非アクティブ化
- 保護動作モードの定義
- アクティベーション方式の設定
- アクティベーション範囲の設定
- 保護の無活動タイムアウトの設定

ゾーン保護のアクティブ化

外部（Cisco Traffic Anomaly Detector Module やその他の手段）から攻撃の兆候が示されてから Guard モジュールを設定してゾーンを保護することも、ゾーンの設定後すぐにゾーンを保護するように Guard モジュールに指示することもできます。Guard モジュールがゾーンを保護する場合、Guard モジュールはゾーンのトラフィックを自分自身に宛先変更し、その保護ポリシーを適用します。

Guard モジュールでゾーンのトラフィック特性をラーニングし終わる前にゾーンが攻撃中になった場合は、オンデマンド保護を使用してゾーンを保護します。新しいゾーンに対する Guard のデフォルトのしきい値を使用すると、効果的なオンデマンド保護を実行できます。詳細については、P.6-45 の「オンデマンド保護のイネーブル化」を参照してください。

（注） 受信トラフィックに応じてゾーン保護をアクティブにするように Guard モジュールを設定する場合は、ゾーン トラフィックを Guard モジュールに手動で宛先変更する必要があります。

ゾーン保護は、次の方法のいずれかでアクティブにできます。

- ゾーン全体の保護。ゾーン設定モードで次のコマンドを入力します。

  protect [**learning**]

  learning キーワードは、ゾーンを保護し、ポリシーのしきい値を調整するように Guard モジュールを設定します。詳細については、P.6-19 の「しきい値の調整」を参照してください。

例

```
user@GUARD-conf-zone-scannet# protect
```

- ゾーンのアドレス範囲の一部である、IP が特定されたゾーンの保護。この場合、Guard モジュールは新しいゾーンを作成します。新しいゾーンの名前は、元になるゾーンの最初の 30 文字と、アンダースコアで連結された特定の IP アドレスで構成されます。同じ名前のゾーンがすでに存在する場合、Guard モジュールは同じ名前の別のゾーンを作成せず、既存のゾーンに対するゾーン保護をアクティブにします。

  IP が特定されたゾーンについてゾーン保護をアクティブにするには、グローバル モードで次のコマンドを入力します。

  protect *zone-name ip-address-general*

  zone-name 引数には、特定のゾーンの名前を指定し、*ip-address-general* 引数には、ゾーンのアドレス範囲内の特定の IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します。たとえば、192.168.5.6 です。

  このゾーンを削除するには、**zone** コマンドの no 形を使用します。

  例

```
user@GUARD# protect scannet 192.168.5.6
creating zone scannet_192.168.5.6
user@GUARD#
```

- 特定の IP アドレスの保護。グローバル モードで次のコマンドを入力します。

  protect *ip-address-general* [*subnet-mask*]

  ip-address-general 引数には、ゾーンのアドレス範囲内にある特定の IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します。たとえば、192.168.5.6 です。Guard モジュールは、IP アドレス アクティベーション方式に従って、ゾーン保護をアクティブにします。詳細については、P.6-41 の「アクティベーション範囲の設定」を参照してください。

複数のゾーンに対して同時に保護関連のコマンドを発行できます。これには、グローバル モードで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてゾーン保護を停止する場合は、グローバル モードで **no protect *** コマンドを入力します。名前が *scan* で始まるゾーン（scannet や scanserver など）すべてについてゾーン保護を停止する場合は、グローバル モードで **no protect** *scan** コマンドを入力します。

ヒント　Guard　モジュールがゾーンのトラフィックを受信していることを確認してください。ゾーン保護をアクティブにしてから少なくとも 10 秒待って、**show rates** コマンドを発行します。レートのうち少なくとも 1 つの値がゼロより大きいことを確認します。すべてのレートの値がゼロの場合は、宛先変更に問題があることを示しています。

ゾーン保護の非アクティブ化

ゾーンに対する攻撃がなく、別のソースを利用してゾーン トラフィックの異常を検出する場合は、ゾーン保護を非アクティブにし、トラフィックの Guard モジュールへの宛先変更を終了してもかまいません。

ゾーン保護を非アクティブにするには、ゾーン設定モードで次のコマンドのいずれかを入力します。

- **no protect**：ゾーン保護を終了します。ゾーンが保護およびラーニング モードの場合、Guard モジュールは継続的にポリシーのしきい値をラーニングします。
- **deactivate**：ゾーン保護と、ラーニング プロセスのしきい値調整フェーズの両方を終了します。

保護動作モードの定義

Guard の保護は、次の 2 つの動作モードにおいてアクティブにできます。

- 自動保護モード：動的フィルタはユーザの操作なしでアクティブになります。これはデフォルトの動作モードです。
- インタラクティブ保護モード：動的フィルタは、インタラクティブ　モードにおいて手動でアクティブになります。動的フィルタは推奨事項としてグループ化され、ユーザの決定を待ちます。ユーザは、これらの推奨事項を確認して、どの推奨事項を受け入れるか、無視するか、自動アクティベーションに切り替えるかを決定できます。

詳細については、第 9 章「インタラクティブ保護モード」を参照してください。

アクティベーション方式の設定

アクティベーション方式は、外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにするゾーンを Guard モジュールが識別する方法を定義します。この兆候には、外部デバイス（Cisco Traffic Anomaly Detector Module など）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）があります。

Guard モジュールは、次のアクティベーション方式をサポートします。

- **ゾーン名**：Guard モジュールは、ゾーン名に基づいてゾーン保護をアクティブにします。ゾーン保護をアクティブにする外部からの兆候には、ゾーン名が含まれている必要があります。これはデフォルトのアクティベーション方式です。
- **IP アドレス**：Guard は、宛先変更されたトラフィックから抽出する情報に基づいて、ゾーン保護をアクティブにします。Guard モジュールは、ゾーンの一部である IP アドレスまたはサブネットで構成された外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。Guard モジュールはゾーンのデータベースをスキャンし、受信 IP アドレスまたはサブネットを含むアドレス範囲を持つゾーンをアクティブにします。受信 IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Guard モジュールは、プレフィックスが最も長く一致するゾーンをアクティブにします。つまり、受信した IP アドレスが含まれていて、アドレス範囲が最も詳細に特定されるゾーンです。受信した IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に全体が含まれている必要があります。

注意　IP アドレスまたはパケットのアクティベーション方式を使用して、同じアドレス範囲を持つ複数のゾーンを設定しないでください。

- **パケット（トラフィック）**：Guard モジュールは、ゾーンを宛先とするトラフィックを受信した場合に、ゾーン保護をアクティブにします。Guard モジュールはゾーンのデータベースをスキャンし、受信パケットの IP アドレスを含むアドレス範囲を持つゾーンをアクティブにします。受信パケットの IP アドレスを含むアドレス範囲を持つ複数のゾーンが設定されている場合、Guard モジュールは、プレフィックスが最も長く一致するゾーンをアクティブにします。つまり、受信パケット IP アドレスを含むアドレス範囲が最も限定的なゾーンがアクティブになります。受信した IP アドレスまたはサブネットは、ゾーンの IP アドレス範囲に全体が含まれている必要があります。

Guard モジュールは、単一の IP アドレスへの受信トラフィックのレートがアクティベーションの詳細度よりも高い場合にのみ、ゾーン保護をアクティブにします。アクティベーションの詳細度はグローバルに定義され、すべてのゾーンに適用されます。

ゾーン保護をアクティブにするのに必要な最小パケット レートを変更するには、設定モードで次のコマンドを入力します。

protect-packet activation-sensitivity *min-rate*

min-rate 引数には、Guard モジュールがゾーンに対するゾーン保護をアクティブにする原因となる、単一のゾーン宛先 IP アドレスを宛先とするパケットの最小レートを定義します。デフォルトは 0 pps です。

（注） アクティベーション範囲がパケットの場合や、Guard モジュールがゾーン トラフィックを監視できない場合は、外部デバイスを使用して、ゾーン トラフィックを Guard モジュールに手動で宛先変更する必要があります。

- **IP アドレスまたはパケット**：Guard モジュールは、ゾーンを宛先とするトラフィック（パケット）を受信した場合、またはゾーンのアドレス範囲の一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。詳細については、上記の箇条書きの **IP アドレス**と**パケット（トラフィック）**の項を参照してください。

アクティベーション方式が **zone-name-only** 以外の場合、Guard モジュールは、ゾーンのアクティベーション範囲に応じて、ゾーン全体または指定された IP アドレス範囲をアクティブにします（P.6-41 の「アクティベーション範囲の設定」を参照）。

アクティベーション方式を設定するには、ゾーン設定モードで次のコマンドを入力します。

activation-interface {**packet** | **ip-address** | **packet-or-ip-address** | **zone-name-only**}

デフォルトは zone-name-only です。ゾーンを複製すると（P.6-7 の「ゾーンの複製」を参照）、ソース ゾーンの設定に関係なく、アクティベーション インターフェイスはデフォルトに設定されます。

（注）アクティベーション範囲が **ip-address-only** で（P.6-41 の「アクティベーション範囲の設定」を参照）、アクティベーション方式が **zone-name-only** 以外の場合は、**protection-end-timer** コマンドを使用して、ゾーンに対する攻撃が終了したことを識別するときに Guard モジュールが使用するタイマーを設定することをお勧めします（P.6-43 の「保護の無活動タイムアウトの設定」を参照）。
protection-end-timer の値が **forever** の場合、Guard モジュールは、ゾーンに対する攻撃が終了したことを識別せず、特定の IP アドレスを保護するために作成したサブゾーンを削除しません。

受信 IP アドレスまたはパケットが他のどのゾーンにも含まれない場合に Guard モジュールが保護するデフォルト ゾーンを作成できます。そのようなゾーンを定義できるのは、ネットワークが同種であるために、同じゾーン テンプレートを使用できる場合のみです。そのゾーンに対してラーニング プロセスを実行することはできません。IP アドレスが 0.0.0.0 で、サブネットが 0.0.0.0 のゾーンを作成します。アクティベーション範囲は、ip-address として定義します（P.6-41 の「アクティベーション範囲の設定」を参照）。

ゾーンのアクティベーション方式を表示するには、**show running-config** コマンドを使用します。

アクティベーション範囲の設定

アクティベーション範囲は、Guard モジュールが外部からの攻撃の兆候を受信した場合に、ゾーン全体またはゾーンの一部に対してゾーン保護をアクティブにするかどうかを定義します。この兆候には、外部デバイス（Cisco Traffic Anomaly Detector Module など）からのコマンドや、ゾーンを宛先とするトラフィック（パケット）があります。

Guard モジュールは、次のアクティベーション範囲をサポートします。

- **ゾーン全体**：ゾーン全体についてゾーン保護をアクティブにします。Guard モジュールは、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合に、ゾーン保護をアクティブにします。

- **IP アドレスのみ**：指定した IP アドレスまたはサブネットに限定してゾーン保護をアクティブにします。Guard モジュールは、ゾーンを宛先とするトラフィックを受信した場合、またはゾーンの一部である IP アドレスまたはサブネットで構成される外部からの攻撃の兆候を受信した場合、新しいゾーン（サブゾーン）を作成します。これはデフォルトのアクティベーション範囲です。詳細については、P.6-42 の「サブゾーンについて」を参照してください。

アクティベーション範囲を設定するには、ゾーン設定モードで次のコマンドを入力します。

activation-extent {**entire-zone** | **ip-address-only**}

デフォルトは ip-address-only です。

ゾーンのアクティベーション範囲を表示するには、**show running-config** コマンドを使用します。

サブゾーンについて

ゾーンの一部（ソース ゾーンのすべての IP アドレス範囲を含まないゾーン）に対してゾーン保護をアクティブにした場合、Guard モジュールはサブゾーンを作成します。サブゾーンの IP アドレス範囲は、ソース ゾーンのアドレス範囲に含まれます。

サブゾーンの設定は、IP アドレスと名前を除いて、ソース ゾーンの設定と同じです。サブゾーンの名前は、ソース ゾーン名の最初の 30 文字と、アンダースコアで連結された IP アドレスおよびサブネットで構成されます。サブゾーンが単一の IP アドレスで構成される場合、サブネットは追加されません。たとえば、ソース ゾーンの名前が *scannet* で、アドレス範囲 *10.10.10.0* とサブネット *255.255.255.0* を持つとき、Guard モジュールが IP アドレス *10.10.10.192* の内部範囲およびサブネット *255.255.255.252* に対してゾーン保護をアクティブにする場合、サブゾーンの名前は *scannet_10.10.10.192_255.255.255.252* となります。

サブゾーンの IP アドレスおよびサブネットは、Guard モジュールが外部からの攻撃の兆候で受信したもの、または Guard モジュールがゾーン保護をアクティブにする原因となったパケットの IP アドレスです。

サブゾーンに対するゾーン保護が終了すると、Guard モジュールはサブゾーンを消去しますが、サブゾーンのログと攻撃レポートは消去しません。サブゾーンのゾーン保護を終了する方法は、通常のゾーンのゾーン保護を終了する方法と同じで、アクティベーション方式と保護の終了のタイムアウトに従います。

Guard モジュールがサブゾーンを消去した後で、サブゾーンのログとレポートを表示するには、次のコマンドを使用します。

- **show log** *sub-zone-name*：詳細については、P.11-2 の「Guard モジュールの設定の表示」を参照してください。
- **show reports** *sub-zone-name* [*report-id* | **current**] [**details**]：詳細については、P.10-14 の「攻撃レポートの表示」を参照してください。

サブゾーンのリストを表示するには、コマンドを入力し、Tab キーを押します。

保護の無活動タイムアウトの設定

Guard モジュールでは、ゾーンに対する攻撃が終了したことを識別した場合、保護およびラーニング モードをアクティブまたは非アクティブにすることができます。Guard モジュールがゾーンを保護している場合、ゾーンに対する攻撃が終了すると、Guard モジュールはゾーン保護を終了します。Guard モジュールが保護およびラーニング モードの場合、Guard モジュールは、攻撃が検出されるとラーニング プロセスを非アクティブにし、ゾーンに対する攻撃が終了するとラーニング プロセスを再開します。

Guard モジュールは、ゾーンに対する攻撃が終了したかどうかを、無活動タイムアウトに従って確認します。このタイムアウトは、数秒から無限まで定義できます。

無活動タイムアウトを定義するには、次のコマンドを入力します。

protection-end-timer {*time-seconds* | **forever**}

表 6-8 に、**protection-end-timer** コマンドの引数とキーワードを示します。

表 6-8　protection-end-timer コマンドの引数とキーワード

パラメータ	説明
time-seconds	タイムアウト（秒単位）。61 以上の整数を入力します。
forever	無限のタイムアウト。

デフォルトは **forever** です。デフォルト値を変更しない場合は、ゾーン保護を手動で非アクティブにする必要があります。

例

```
user@GUARD-conf-zone-scannet# protection-end-timer 300
```

Guard モジュールは、動的フィルタの無活動とドロップされたトラフィックに基づいて、無活動を測定します。事前に定義された期間に、動的フィルタが使用されず、次の条件が両方とも当てはまる場合、Guard モジュールはゾーンに対する攻撃が終了したものと見なします。

- 新しい動的フィルタが追加されない：動的フィルタを削除する時期を Guard が決定する方法については、P.7-38 の「動的フィルタの非アクティブ化」を参照してください。
- ドロップされているゾーン　トラフィックのレートが定義済みのしきい値よりも低い：Guard モジュールは、保護メカニズム（動的フィルタ、フレックスコンテンツ フィルタ、およびレート リミット モジュール）によって攻撃の一部と識別されたゾーン パケットをドロップします。ドロップされるパケットは、ゾーンの Dropped カウンタを使用してカウントされます（詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照）。デフォルトのしきい値は 1 pps です。ドロップ カウンタのしきい値を変更するには、ゾーン設定モードで次のコマンドを入力します。

  attack-detection zone-malicious-rate *threshold*

  threshold 引数には、ドロップされるゾーン パケットの最小レートを定義します。レートがこのしきい値より低くなった場合、Guard モジュールがゾーン保護を終了することがあります。

ゾーンのアクティベーション方式が**パケット**の場合、Guard モジュールは、ゾーンを非アクティブにする前に、受信トラフィックに基づいて無活動を確認します。Guard モジュールが保護を非アクティブにするのは、前の条件が当てはまり、ゾーンへのパケットが受信されなかった場合のみです。

オンデマンド保護のイネーブル化

ゾーンが攻撃にさらされている場合など、緊急を要する場合には、ラーニング プロセスを実行せずにゾーンを保護することができます。システム定義のゾーン テンプレートには、ラーニング プロセスが完了していないゾーンの保護に適した定義済みの保護ポリシーとユーザ フィルタが含まれています。このゾーン テンプレートのデフォルトのしきい値は、Guard モジュールがゾーンのトラフィックに異常を発見した場合にスプーフィング防止メカニズムをすぐにアクティブにするように調整されています。

Guard モジュールはゾーンのトラフィック パターンについての知識を持たないため、送信元 IP アドレスをブロック（ドロップ）するために使用されるしきい値は、比較的高い値に設定されています。つまり、オンデマンド保護では、スプーフィングを利用しない攻撃を軽減する場合にはユーザの介入が必要になります。ゾーンの正当なトラフィックと悪意のあるトラフィックのレートを監視して、Guard モジュールの軽減アクションを確認する必要があります。

次のいずれかの場合は、ゾーンに対してオンデマンド保護が必要になる場合があります。

- ゾーンがラーニング プロセスの実行中である。
- Guard モジュールが保護およびラーニング モードになっているが、ゾーンのトラフィック特性をラーニングしていない。
- ゾーンのトラフィックを表さないと考えられるポリシーのしきい値を受け入れている。

オンデマンド保護を開始するには、次の手順を実行します。

ステップ 1　新しいゾーンを作成します。次のコマンドを入力します。

```
zone new-zone-name [template-name] [interactive]
```

詳細については、P.6-4 の「新しいゾーンの作成」を参照してください。

ステップ 2　ゾーンの IP アドレスを定義します。次のコマンドを入力します。

```
ip address ip-addr [ip-mask]
```

詳細については、P.6-9 の「ゾーンのアトリビュートの設定」を参照してください。

ステップ 3　ゾーン保護をアクティブにします。次のコマンドを入力します。

```
protect
```

詳細については、P.6-35 の「ゾーンの保護」を参照してください。

ステップ 4　ゾーンのトラフィック パターンを分析します。詳細については、第 13 章「Guard モジュールによる軽減の分析」を参照してください。

CHAPTER 7

ゾーンのフィルタの設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）フィルタの設定方法について説明します。

この章は、次の項で構成されています。

- 概要
- フレックスコンテンツ フィルタの設定
- バイパス フィルタの設定
- ユーザ フィルタの設定
- 動的フィルタの設定

概要

ゾーン フィルタは、Guard が特定のトラフィック フローを処理する方法を定義します。ユーザは、フィルタを設定して、カスタマイズされたトラフィック誘導や DDoS 攻撃の防止メカニズムをさまざまに設計することができます。

Guard モジュールでは、次のタイプのフィルタが使用されます。

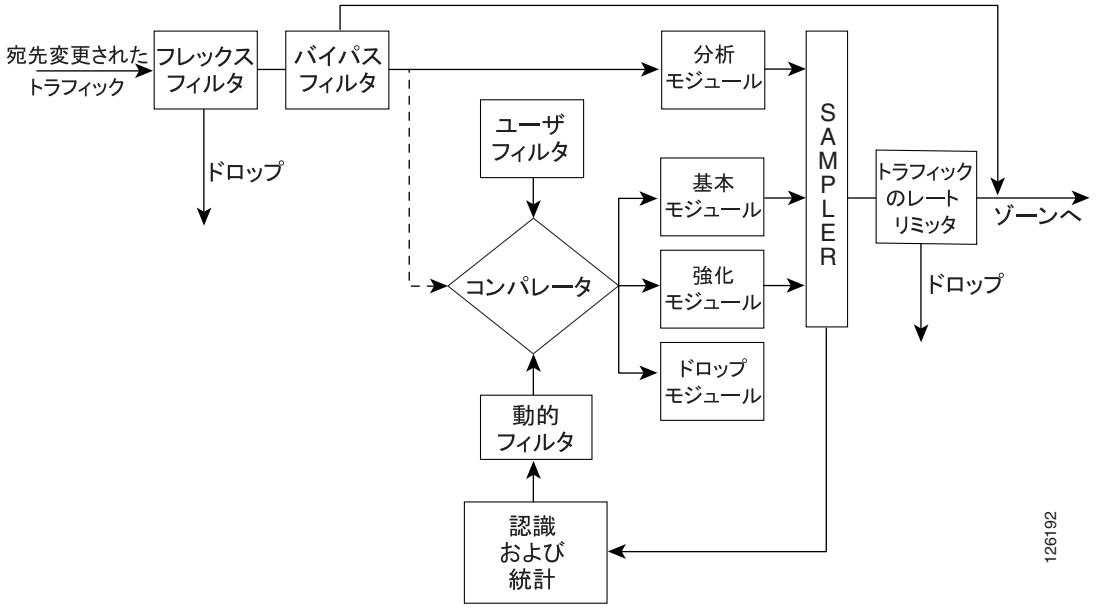
- **ユーザ フィルタ**：ユーザ フィルタは、特定のトラフィック フローを関連する Guard の保護モジュールに誘導します。このフィルタは、異常なトラフィックや悪意のあるトラフィックが検出されたときに Guard が最初に実行するアクションを定義します。ゾーン設定には、多様なタイプの攻撃を処理できるオンデマンドの保護用に設定された、デフォルトのユーザ フィルタのセットが含まれています。ユーザ フィルタを変更すると、Guard の保護モジュールの機能をカスタマイズし、攻撃の疑いがある場合のトラフィック フロー処理規則を設定できます。詳細については、P.7-24 の「ユーザ フィルタの設定」を参照してください。
- **バイパス フィルタ**：バイパス フィルタは、特定のトラフィック フローが Guard の保護メカニズムによって処理されないように防止します。

  信頼されたトラフィックが Guard の保護メカニズムを通らないように誘導し、そのトラフィックを直接ゾーンに転送できます。

  詳細については、P.7-21 の「バイパス フィルタの設定」を参照してください。
- **フレックスコンテンツ フィルタ**：フレックスコンテンツ フィルタは、特定のトラフィック フローをカウントまたはドロップします。フレックスコンテンツ フィルタは、バークリー パケット フィルタとパターン フィルタを組み合せたもので、IP ヘッダーと TCP ヘッダーのフィールドに基づいたフィルタリングやペイロード コンテンツに基づいたフィルタリングなどの非常に柔軟なフィルタリング機能、および複雑なブール式をユーザに提供します。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」を参照してください。
- **動的フィルタ**：動的フィルタは、特定のトラフィック　フローを関連する Guard の保護モジュールに誘導します。Guard は、トラフィック フローを分析した結果として動的フィルタを作成します。この一連のフィルタは、ゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整されます。動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。詳細については、P.7-31 の「動的フィルタの設定」を参照してください。

図 7-1 に、Guard モジュールのフィルタ システムを示します。

図 7-1　Guard モジュールのフィルタ システム



ユーザのアクションや、リモートのネットワーク検知 DDoS 要素（Cisco Traffic Anomaly Detector Module など）によってゾーンの保護がイネーブルになると、Guard はゾーンのトラフィックを分析します。

Guard は、ゾーンに流れるトラフィックのレートを監視します。定義済みのレートを超過するトラフィックはドロップされ、正当なトラフィックはゾーンに転送されます。Guard は、ゾーンのトラフィックの統計分析を行い、クローズドループのフィードバック サイクルを制御して、動的に変化するゾーンのトラフィック特性や変化する DDoS 攻撃のタイプに合せて保護措置を調整します。

トラフィック フローの統計分析を行うために、Guard は、特定のトラフィック タイプの処理に関する定義を持っています。これらの定義をポリシーといいます。ポリシーは、トラフィック フローを持続的に測定し、特定のトラフィック フローが悪意のあるものまたは異常であると判断すると、そのフローに対してアクションを実行します。このアクションは、フローがポリシーのしきい値を超過すると発生します。

Guard モジュールは異常なトラフィックを識別すると、次のように動作します。

1. 攻撃を処理するアクションが設定された動的フィルタの作成を開始する。Guard モジュールは、デフォルトでは、すべてのトラフィックをユーザ フィルタに誘導する最初の動的フィルタを追加します。Guard モジュールが十分な時間をかけて攻撃を分析するまでの間、ユーザ フィルタは新たに発生する DDoS 攻撃に対して最初の防御策を提供します。
2. Guard モジュール内部のトラフィック フローを変更する。異常なトラフィックは、破線で示されているように、コンパレータに流れます。コンパレータは、動的フィルタとユーザ フィルタから入力を受け取ります。コンパレータは、フローに一致する最初のユーザ フィルタを動的フィルタと比較し、提案された中で最も強力な保護措置を選択します。そして、認証のためにトラフィックを関連する保護モジュールに誘導します。

動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。デフォルトでは、ユーザがゾーンの保護を非アクティブにするまで Guard モジュールはゾーンを保護します。

フィルタのトラフィック フロー

フィルタが処理するトラフィック フローを設定する必要があります。表 7-1 に、フィルタのフローの引数を説明します。

詳細については、「バイパス フィルタの設定」、「ユーザ フィルタの設定」、および「動的フィルタの設定」の各項を参照してください。

表 7-1　フィルタのフローの引数

パラメータ	説明
src-ip	特定の IP アドレスからのフローを処理します。すべての IP アドレスを示すには、アスタリスク（*）を使用します。
ip-mask	（オプション）特定のサブネットからのフローを処理します。サブネット マスクには、クラス C の値のみを指定できます。デフォルトのサブネットは、255.255.255.255 です。

表 7-1　フィルタのフローの引数（続き）

パラメータ	説明
protocol	特定のプロトコルのフローを処理します。すべてのプロトコルを示すには、アスタリスク（*）を使用します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
dest-port	特定の宛先ポートに向かうトラフィックを処理します。すべての宛先ポートを示すには、アスタリスク（*）を使用します。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
fragments-type	（オプション）断片化されたトラフィックをフィルタが処理するかどうかを指定します。断片化のタイプは、次のとおりです。 • **no-fragments**：断片化されていないトラフィック • **fragments**：断片化されたトラフィック • **any-fragments**：断片化されたトラフィックと断片化されていないトラフィック デフォルトは、**no-fragments** です。

表 7-2 に、フィルタの **show** コマンドのフィールドを説明します。

詳細については、「バイパス フィルタの表示」、「ユーザ フィルタの表示」、および「動的フィルタの表示」を参照してください。

表 7-2　フィルタの show コマンドのフィールドの説明

フィールド	説明
Source IP	フィルタが処理するトラフィックの送信元 IP アドレスを指定します。
Source Mask	フィルタが処理するトラフィックの送信元アドレスのマスクを指定します。
Proto	フィルタが処理するトラフィックのプロトコル番号を指定します。
DPort	フィルタが処理するトラフィックの宛先ポートを指定します。
Frg	フィルタが断片化されたトラフィックを処理するかどうかを指定します。 • **yes**：フィルタは断片化されたトラフィックを処理します。 • **no**：フィルタは断片化されていないトラフィックを処理します。 • **any**：フィルタは、断片化されたトラフィックと断片化されていないトラフィックの両方を処理します。

送信元 IP アドレス、送信元アドレスのマスク、プロトコル番号、および宛先ポートは、特定のものでなくてもかまいません。アスタリスク（*）は、フィルタがすべてのフィールド値に対して動作するか、フィルタに複数の値が一致したことを示します。

フレックスコンテンツ フィルタの設定

フレックスコンテンツ フィルタを使用すると、パケット ヘッダーのフィールドまたはパケット ペイロードのパターンに基づいて、ゾーン トラフィックをフィルタリングできます。着信トラフィックに現れているパターンに基づいて攻撃を識別できます。それらのパターンでは、既知のワームまたは一定のパターンを持つフラッド攻撃が識別可能です。ただし、フレックスコンテンツ フィルタはリソースを大量に消費します。フレックスコンテンツ フィルタはパフォーマンスに影響を及ぼす可能性があるため、十分に注意して使用することをお勧めします。特定のポートに送信される TCP トラフィックなど、動的フィルタによって識別できる特定の攻撃からの保護にフレックスコンテンツ フィルタを使用する場合は、動的フィルタを使用してトラフィックをフィルタリングすることをお勧めします。

フレックスコンテンツ フィルタは、目的のパケット フローをカウントまたはドロップする場合、および特定の悪意のあるトラフィックの送信元を識別する場合に使用します。

フレックスコンテンツ フィルタは、バークリー パケット フィルタとパターン フィルタを組み合せたもので、豊富なフィルタリング機能を持っています。

この項では、次のトピックについて取り上げます。

- フレックスコンテンツ フィルタの追加
- TCPDump 式の構文について
- パターン式の構文について
- フレックスコンテンツ フィルタの表示
- フレックスコンテンツ フィルタの削除
- フレックスコンテンツ フィルタの状態の変更

フレックスコンテンツ フィルタの追加

フレックスコンテンツ フィルタは、行番号の昇順でアクティブになります。したがって、新しいフレックスコンテンツ フィルタを追加する場合には、リストの適切な位置に配置することが重要です。

トラフィックが drop アクションを持つフレックスコンテンツ フィルタに一致すると、Guard モジュールはフレックスコンテンツ フィルタのアクティブ化を停止します。

フレックスコンテンツ フィルタを設定するには、次の手順を実行します。

ステップ 1　フレックスコンテンツ　フィルタのリストを表示して、リスト内で新しいフィルタを追加する位置を確認します。詳細については、P.7-18 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　現在の行番号が連続したものである場合は、新しいフレックスコンテンツ　フィルタを挿入できるようにフレックスコンテンツ フィルタの番号を順に増加させます。次のコマンドを入力します。

```
flex-content-filter renumber [start [step]]
```

表 7-3 に、**flex-filter renumber** コマンドの引数を示します。

表 7-3　flex-filter renumber コマンドの引数

パラメータ	説明
start	（オプション）フレックスコンテンツ フィルタ リストの新しい開始番号を示す 1 ～ 9,999 の整数。デフォルトは 10 です。
step	（オプション）フレックスコンテンツ フィルタの各行番号の増分を指定する 1 ～ 999 の整数。デフォルトは 10 です。

ステップ 3　（オプション）進行中の攻撃または以前記録した攻撃のパターン式をフィルタリングする場合、Guard モジュールをアクティブ化し、**show packet-dump signatures** コマンドを使用して攻撃のシグニチャを生成することができます。詳細については、P.11-28 の「パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成」を参照してください。

ステップ 4　新しいフレックスコンテンツ　フィルタを追加します。次のコマンドを入力します。

```
flex-content-filter row-num {disabled | enabled} {drop | count}
protocol port [start start-offset [end end-offset]] [ignore-case]
expression tcpdump-expression pattern pattern-expression
```

表 7-4 に、**flex-filter** コマンドの引数とキーワードを示します。

表 7-4　flex-filter コマンドの引数とキーワード

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号。行番号はフィルタの ID で、これによって複数のフレックスコンテンツ フィルタの優先順位が定義されます。Guard モジュールは、行番号の昇順でフィルタを操作します。
disabled	フィルタの状態をディセーブルに設定します。フィルタはトラフィックに関連付けられません。
enabled	フィルタの状態をイネーブルに設定します。フィルタはトラフィックに関連付けられ、一致が検出されるとアクションを実行します。 これがデフォルトの状態です。
drop	フィルタに一致するフローをドロップします。
count	フィルタに一致するフローをカウントします。

表 7-4　flex-filter コマンドの引数とキーワード（続き）

パラメータ	説明
protocol	特定のプロトコルのフローを処理します。すべてのプロトコルを示すには、アスタリスク（*）を使用します。0 ～ 255 の整数を入力します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
port	特定の宛先ポートに向かうトラフィックを処理します。0 ～ 65,535 の整数を入力します。特定のポート番号を定義するには、特定のプロトコル番号を定義する必要があります。 すべての宛先ポートを示すには、アスタリスク（*）を使用します。プロトコル番号を 6（TCP）または 17（UDP）に設定する場合のみ、アスタリスクを使用できます。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
start-offset	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット（バイト単位）。デフォルトは 0（ペイロードの先頭）です。このオフセットは、*pattern* フィールドに適用されます。0 ～ 1800 の整数を入力します。 **show packet-dump signatures** コマンドの出力からパターンをコピーする場合は、この引数をコマンドの出力の Start Offset フィールドからコピーします。

表 7-4　flex-filter コマンドの引数とキーワード（続き）

パラメータ	説明
end-offset	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット（バイト単位）。デフォルトは、パケット長（ペイロードの末尾）です。このオフセットは、*pattern* フィールドに適用されます。0 ～ 1800 の整数を入力します。 **show packet-dump signatures** コマンドの出力からパターンをコピーする場合は、この引数をコマンドの出力の End Offset フィールドからコピーします。
ignore-case	*pattern-expression* 引数で大文字と小文字が区別されないようにします。 デフォルトでは、*pattern-expression* 引数では大文字と小文字が区別されます。
tcpdump-expression	パケットと照合する式を指定します。式はバークリー パケット フィルタの形式です。詳細および設定の例については、P.7-13 の「TCPDump 式の構文について」を参照してください。 式にスペースが含まれる場合は、式を引用符で囲みます。 空の式を入力するには、二重引用符（“ “）を使用します。 式に引用符を含めるには、バックスラッシュ（\）をエスケープ文字として使用します。 TCPDump 式の構文については、ヘルプを使用できません。

表 7-4　flex-filter コマンドの引数とキーワード（続き）

パラメータ	説明
pattern-expression	パケット ペイロードと照合する正規表現のデータ パターンを指定します。詳細については、P.7-16 の「パターン式の構文について」を参照してください。 Guard モジュールをアクティブ化し、**show packet-dump signatures** コマンドを使用してシグニチャを生成することができます。P.11-28 の「パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成」を参照してください。 式にスペースが含まれる場合は、式を引用符で囲みます。 空の式を入力するには、二重引用符（“ “）を使用します。 式に引用符を含めるには、バックスラッシュ（\）をエスケープ文字として使用します。 パターン式の構文については、ヘルプを使用できません。

フレックスコンテンツ フィルタは、次の順序でフィルタリング基準を適用します。

- フレックスコンテンツ フィルタは最初に、*protocol* および *port* に基づいてパケットをフィルタリングする。
- 次に、*tcpdump-expression* を適用する。
- フレックスコンテンツ フィルタは、残りのパケットに対して *pattern-expression* を使用してパターン マッチングを実行する。

フィルタの状態はいつでも変更できます。詳細については、P.7-20 の「フレックスコンテンツ フィルタの状態の変更」を参照してください。

フィルタ アクションはいつでも変更できます。詳細については、P.7-19 の「フレックスコンテンツ フィルタの削除」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression "ip[6:2] & 0x1fff=0" pattern
"/ HTTP/1\.1\ x0D\0AAccept: .*/.*\x0D\x0AAccept-Language:
en*\x0D\x0AAccept-Encoding: gzip, deflate\x0D\x0AUser-Agent:
Mozilla/4\.0"
```

TCPDump 式の構文について

TCPDump 式は、パケットを照合する式を指定します。式はバークリー パケット フィルタの形式です。

（注） 宛先ポートとプロトコルに基づいてトラフィックをフィルタリングする場合は、tcpdump の式を使用できます。ただし、パフォーマンスへの影響を考慮し、これらの基準でトラフィックをフィルタリングする場合は、フレックスコンテンツ フィルタで *protocol* 引数と *port* 引数を使用することをお勧めします。

表 7-5 に、フレックスコンテンツ フィルタの式のパラメータの説明を示します。

表 7-5　フレックスコンテンツ フィルタのパラメータ

パラメータ	説明
dst host *host_ip_address*	宛先ホスト IP アドレスへのトラフィック。
src host *host_ip_address*	送信元ホスト IP アドレスからのトラフィック。
host *host_ip_ address*	送信元および宛先の両方のホスト IP アドレスの間のトラフィック。
net *net* mask *mask*	特定のネットワークへのトラフィック。
net *net/len*	特定のサブネットへのトラフィック。
dst port *destination_port_number*	宛先ポート番号への TCP または UDP トラフィック。
src port *source_port_number*	送信元ポート番号からの TCP または UDP トラフィック。

表 7-5　フレックスコンテンツ フィルタのパラメータ（続き）

パラメータ	説明
port *port_number*	送信元および宛先の両方のポート番号間の TCP または UDP トラフィック。
less *packet_length*	特定のバイト長以下の長さを持つパケット。
greater *packet_length*	特定のバイト長以上の長さを持つパケット。
ip proto *protocol*	ICMP、UDP、または TCP のプロトコル番号を持つパケット。
ip broadcast	ブロードキャスト IP パケット。
ip multicast	マルチキャスト パケット。
ether proto *protocol*	IP、ARP、または RARP などの特定のプロトコル番号またはプロトコル名を持つイーサネット プロトコル パケット。
expr relop expr	特定の式に適合するトラフィック。詳細については、表 7-6 を参照してください。

表 7-6 に、フレックスコンテンツ フィルタの式の規則の説明を示します。

表 7-6　フレックスコンテンツ フィルタの式の規則

式の規則	
relop	>、<、>=、<=、=、!=
expr	整数の定数（標準の C 構文で表現されたもの）、通常のバイナリ演算子（+、-、*、/、&、|）、長さ演算子、および特殊なパケット データ アクセスで構成される算術式。パケット内のデータにアクセスするには、次の構文を使用します。 *proto* [*expr*: *size*]

表 7-6　フレックスコンテンツ フィルタの式の規則（続き）

式の規則	
proto	インデックス操作用のプロトコル層を指定します。指定可能な値は、**ether**、**ip**、**tcp**、**udp**、または **icmp** です。指定されたプロトコル層までの相対的なバイト オフセットは、*expr* で指定されます。*size* 引数はオプションです。目的のフィールドのバイト数を示し、1、2、または 4 になります。デフォルトは 1 です。*len* 引数には、パケットの長さを指定します。

次の方法により、プリミティブを組み合せることができます。

- プリミティブとオペレータを小カッコで囲んだグループ（小カッコはシェルの特殊文字であるため、エスケープする必要があります）。
- 否定：**!** または **not** を使用します。
- 連結：**&&** または **and** を使用します。
- 代替：**||** または **or** を使用します。

否定は、最も高い優先度を持ちます。代替と連結の優先順位は同じで、左から右に関連付けられます。連結には、並置ではなく、明示的な **and** トークンが必要です。キーワードなしで識別子を指定した場合は、最後に指定されたキーワードが使用されます。

バークリー パケット フィルタの設定オプションの詳細については、http://www.freesoft.org/CIE/Topics/56.htm を参照してください。

次の例は、断片化されていないデータグラムと断片化されたデータグラムのフラグメント 0 のみをカウントする方法を示しています。このフィルタは、TCP と UDP のインデックス操作に暗黙的に適用されます。たとえば、tcp[0] は常に TCP ヘッダーの最初のバイトを意味し、中間のフラグメントの最初のバイトを意味することはありません。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression ip[6:2]&0x1fff=0 pattern ""
```

次の例は、すべての TCP RST パケットをドロップする方法を示しています。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled drop * *
expression tcp[13]&4!=0 pattern ""
```

次の例は、エコー要求およびエコー応答（ping）ではないすべての ICMP パケットをカウントする方法を示しています。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression "icmp [0]!=8 and icmp[0] != 0" pattern ""
```

次の例は、ポート 80 を宛先とし、ポート 1000 を送信元としないすべての TCP パケットをカウントする方法を示しています。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * *
expression "tcp and dst port 80 and not src port 1000" pattern ""
```

パターン式の構文について

パターン（正規表現）は、一連の文字を含んだ文字列を記述したものです。パターンには、パターンの要素を実際に列挙するのではなく、一連の文字列を記述します。パターンは、一般文字と特殊文字で構成されます。一般文字には、特殊文字とは見なされない印刷可能な ASCII 文字が含まれます。特殊文字は、どのようなマッチングを実行するのかを示します。フレックスコンテンツ フィルタは、このパターンをパケットの内容（パケットのペイロード）と照合します。たとえば、*version 3.1*、*version 4.0*、および *version 5.2* の 3 つの文字列は、*version* .*\.* というパターンで記述されます。

特殊文字とは、特殊な意味を持つ文字で、Guard モジュールが式に対してどのような照合を実行するのかを指定する文字です。表 7-7 で、使用できる特殊文字について説明します。

表 7-7　フレックスコンテンツ パターン フィールドの説明

特殊文字	説明
.*	0 個またはそれ以上の文字を含んでいる文字列と一致します。たとえば、パターン *goo.*s* は *goos*、*goods*、*good for ddos* などと一致します。
\	特殊文字が持つ特殊な意味を取り除きます。特殊文字を文字列の中で 1 つの文字パターンとして使用するには、各文字の先頭にバックスラッシュ（\）を入力して特殊な意味を取り除きます。たとえば、シーケンス \\ は \ と一致し、シーケンス \. は . と一致します。 文字として使用するアスタリスク（*）の前にもバックスラッシュを配置する必要があります。
\xHH	16 進値と一致します。H は 16 進数の数字で、大文字と小文字は区別されません。16 進値は 2 桁で入力する必要があります。たとえば、\x41 は A と一致します。

デフォルトでは、パターンでは大文字と小文字が区別されます。パターン式で大文字と小文字が区別されないようにするには、**ignore-case** キーワードを使用します。P.7-8 の「フレックスコンテンツ フィルタの追加」を参照してください。

次の例は、パケットのペイロードに特定のパターンが含まれているパケットをドロップする方法を示しています。この例のパターンは、Slammer ワームから抽出されたものです。プロトコル、ポート、および tcpdump 式は特定のものでなくてもかまいません。

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled drop * *
expression " " pattern
\x89\xE5Qh\.dllhel32hkernQhounthickChGetTf\xB911
Qh32\.dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

フレックスコンテンツ フィルタの表示

フレックスコンテンツ フィルタを表示するには、ゾーン設定モードで次のコマンドを入力します。

show flex-content-filters

表 7-8 に、**show flex-content-filters** コマンドの出力フィールドを示します。

表 7-8　show flex-content-filters コマンドのフィールドの説明

フィールド	説明
Row	フレックスコンテンツ フィルタの優先順位を示します。
State	フィルタの状態（イネーブルまたはディセーブル）を示します。
Action	フィルタが特定のトラフィック タイプに対して実行するアクションを示します。
Protocol	フィルタが処理するトラフィックのプロトコル番号を指定します。
Port	フィルタが処理するトラフィックの宛先ポートを指定します。
Start	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセットを指定します（バイト単位）。（このオフセットは、*pattern* フィールドに適用されます）。
End	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセットを指定します（バイト単位）。（このオフセットは、*pattern* フィールドに適用されます）。
Match-case	フィルタが一致するパターンで大文字と小文字が区別されるかどうかを示します（この引数は、*pattern* フィールドに適用されます）。 yes の場合は大文字と小文字が区別され、no の場合は区別されません。

表 7-8　show flex-content-filters コマンドのフィールドの説明（続き）

フィールド	説明
TCPDump-expression	パケットと照合する式をバークリー パケット フィルタ形式で指定します。TCPDump 式の構文については、P.7-13 の「TCPDump 式の構文について」を参照してください。
Pattern-filter	パケット ペイロードと照合する正規表現のデータパターンを指定します。パターン フィルタの構文については、P.7-16 の「パターン式の構文について」を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィック レートを pps で示します。

フレックスコンテンツ フィルタの削除

フレックスコンテンツ フィルタを削除できます。または、フレックスコンテンツ フィルタをディセーブルにして、Guard モジュールがフィルタの式に基づいてパケットをフィルタリングしないように設定できます。詳細については、P.7-20 の「フレックスコンテンツ フィルタの状態の変更」を参照してください。

フレックスコンテンツ フィルタを削除するには、次の手順を実行します。

ステップ 1　フレックスコンテンツ　フィルタのリストを表示し、削除するフレックスコンテンツ フィルタの行番号を確認します。詳細については、P.7-18 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　フレックスコンテンツ フィルタを削除します。次のコマンドを入力します。

```
no flex-content-filter row-num
```

row-num 引数には、フレックスコンテンツ フィルタの行番号を指定します。すべてのフレックスコンテンツ フィルタを削除するには、アスタリスク（*）を入力します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# no flex-content-filters 5
```

フレックスコンテンツ フィルタの状態の変更

フレックスコンテンツ フィルタの状態を変更できます。フレックスコンテンツ フィルタをディセーブルにして、Guard モジュールがフィルタの式に基づいてパケットをフィルタリングしないように設定できます。フィルタは Guard モジュールのフレックスコンテンツ フィルタ リストに残ったままになります。このようにして、ある種類のトラフィックに対する Guard モジュールのフィルタリングを停止することができます。その後で、もう一度指定されたトラフィックをフィルタリングするように Guard モジュールを設定できます。このとき、フィルタを再設定する必要はありません。また、フレックスコンテンツ フィルタを削除することもできます。詳細については、P.7-19 の「フレックスコンテンツ フィルタの削除」を参照してください。

フレックスコンテンツ フィルタの状態を変更するには、次の手順を実行します。

ステップ 1　フレックスコンテンツ　フィルタのリストを表示し、状態を変更するフレックスコンテンツ フィルタの行番号を確認します。詳細については、P.7-18 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　フレックスコンテンツ　フィルタの状態を変更します。次のコマンドを入力します。

flex-content-filter *row-num* {**disabled** | **enabled**}

row-num 引数には、フレックスコンテンツ フィルタの行番号を指定します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# flex-content-filters 5 disabled
```

バイパス フィルタの設定

バイパス フィルタは、Guard の保護メカニズムを利用しない保護ポリシーの採用をサポートするためのフィルタです。バイパス フィルタは、Guard の動的フィルタ、分析、基本、強化の各保護モジュール、およびレート リミット保護モジュールで特定のトラフィック フローを処理しないようにする場合に使用します。たとえば、信頼されたトラフィック フローについては、スプーフィング防止メカニズムおよびゾンビ防止メカニズムを含めて Guard の保護モジュールをバイパスするように指定できます。バイパス フィルタを使用すると、信頼されたトラフィックを Guard の保護メカニズムの対象から除外して、ゾーンに直接送信できるようになります。

（注） バイパス フィルタで処理されるトラフィックは、レート リミット モジュールを経由しません。

この項では、次のトピックについて取り上げます。

- バイパス フィルタの追加
- バイパス フィルタの表示
- バイパス フィルタの削除

バイパス フィルタの追加

バイパス フィルタを追加するには、関連するゾーン設定モードで次のコマンドを入力します。

bypass-filter *row-num* ***src-ip*** [***ip-mask***] ***protocol dest-port*** [***fragments-type***]

表 7-9 に、**bypass-filter** コマンドの引数を示します。

表 7-9　bypass-filter コマンドの引数

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号を割り当てます。行番号はフィルタの ID で、これによって複数のバイパス フィルタの優先順位が定義されます。Guard モジュールは、行番号の昇順でフィルタを操作します。
フローの引数とキーワード	フィルタリングを実行する対象のフロー。*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 7-1 を参照してください。

（注） fragments-type と dest-port を両方指定することはできません。fragments-type を設定する場合は、dest-port に * を入力してください。

バイパス フィルタの表示

バイパス フィルタを表示するには、関連するゾーン設定モードで次のコマンドを入力します。

show bypass-filters

表 7-10 に、**show bypass-filters** コマンドの出力フィールドを示します。

表 7-10　show bypass-filters コマンドのフィールドの説明

フィールド	説明
Row	バイパス フィルタの優先順位を示します。
Filter flow	フィルタリングを実行する対象のフローを示します。Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 7-2 を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィックレートを pps で示します。

バイパス フィルタの削除

バイパス フィルタを削除するには、次の手順を実行します。

ステップ 1　バイパス フィルタのリストを表示し、削除するバイパス フィルタの行番号を確認します。詳細については、前の項、「バイパス フィルタの表示」を参照してください。

ステップ 2　バイパス フィルタを削除します。次のコマンドを入力します。

```
no bypass-filter row-num
```

row-num 引数には、バイパス フィルタの行番号を指定します。すべてのバイパス フィルタを削除するには、アスタリスク（*）を入力します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# no bypass-filter 10
```

ユーザ フィルタの設定

ユーザ フィルタは、特定のトラフィック フローを関連する Guard の保護モジュールに誘導します。このフィルタは、異常なトラフィックや悪意のあるトラフィックが検出されたときに Guard が最初に実行するアクションを定義します。

ゾーン設定には、多様なタイプの攻撃を処理できるオンデマンドの保護用に設定された、デフォルトのユーザ フィルタのセットが含まれています。ユーザ フィルタを変更すると、Guard の保護モジュールの機能をカスタマイズし、攻撃の疑いがある場合の Guard による特定のトラフィック フローの処理規則を設定できます。ユーザ フィルタは、特定のトラフィック フローを関連する保護モジュール、およびスプーフィング防止メカニズムやゾンビ防止メカニズムに誘導したり、ドロップしたりできます。

Guard は、ゾーンが宛先になっているトラフィックを継続的に分析します。異常なトラフィック パターンを検出すると、攻撃の処理方法を定義する動的フィルタの作成を開始します。Guard モジュールは、デフォルトでは、すべてのトラフィックをユーザ フィルタに誘導する最初の動的フィルタを追加します。Guard モジュールが十分な時間をかけて攻撃を分析するまでの間、ユーザ フィルタは新たに発生する DDoS 攻撃に対して最初の防御策を提供します。

Guard モジュールはユーザ フィルタと動的フィルタの両方を調べた後で、当該トラフィック フローの処理方法を決定します。コンパレータは、フローに一致する最初のユーザ フィルタを動的フィルタと比較し、提案された中で最も強力な保護措置を選択します。そして、認証のためにトラフィックを関連する保護モジュールに誘導します。動的フィルタまたはユーザ フィルタが実行するアクションは、重大度レベルの大きい順に、drop、strong、basic、permit です。アクション redirect/zombie および block-unauthenticated が指定された動的フィルタは、同じタイプのトラフィックを処理するユーザ フィルタがあっても適用されます。動的フィルタは Guard モジュールの認証メカニズムに影響しますが、トラフィック フローには直接影響を及ぼさないためです。

ユーザ フィルタは、行番号の昇順でアクティブになります。したがって、新しいユーザ フィルタを追加する場合には、リストの適切な位置に配置することが重要です。

表 7-11 に、ユーザ フィルタで実行可能なアクションを説明します。

表 7-11　ユーザ フィルタのアクション

アクション	説明
permit	フローの統計分析を行わないよう、また、スプーフィング防止やゾンビ防止の保護メカニズムがこのフローを処理しないよう防止する場合に使用します。このフローは他の保護メカニズムによって処理されないため、このフィルタにはレート リミットとバースト リミットを設定することをお勧めします。
basic/redirect	HTTP 経由のアプリケーションを認証する場合に使用します。
basic/reset	TCP 経由のアプリケーションを認証する場合に使用します。HTTP トラフィック フローには basic/redirect のアクションを実行することをお勧めします。
basic/default	TCP 経由でないトラフィック フローを認証する場合に使用します。
basic/dns-proxy	TCP DNS トラフィック フローを認証する場合に使用します。
basic/safe-reset	TCP 接続のリセットを許容しない TCP アプリケーション トラフィック フローを認証する場合に使用します。HTTP トラフィック フローには basic/redirect のアクションを実行することをお勧めします。
drop	トラフィック フローをドロップする場合に使用します。
strong	トラフィック フローの強化認証が必要な場合や、それまでのフィルタが該当アプリケーションに適していないと考えられる場合に使用します。認証は、各接続に対して行われます。 TCP 着信接続については Guard モジュールがプロキシの役割を果たすため、このアクションは、Access Control List（ACL; アクセス コントロール リスト）を使用しているなど、ネットワークが IP アドレスに従って管理される場合、このような接続に使用しないことをお勧めします。

この項では、次のトピックについて取り上げます。

- ユーザ フィルタの追加
- ユーザ フィルタの表示
- ユーザ フィルタの削除

ユーザ フィルタの追加

ユーザ フィルタを追加するには、次の手順を実行します。

ステップ 1　ユーザ フィルタのリストを表示して、リスト内で新しいフィルタを追加する位置を確認します。詳細については、P.7-28 の「ユーザ フィルタの表示」を参照してください。

ステップ 2　現在の行番号が連続したものである場合は、新しいユーザ フィルタを挿入できるようにユーザ フィルタの番号を順に増加させます。次のコマンドを入力します。

```
user-filter renumber [start [step]]
```

表 7-12 に、**user-filter renumber** コマンドの引数を示します。

表 7-12　user-filter renumber コマンドの引数

パラメータ	説明
start	（オプション）ユーザ フィルタ リストの新しい開始番号を示す 1 ～ 9,999 の整数。デフォルトは 10 です。
step	（オプション）ユーザ フィルタの各行番号の増分を指定する 1 ～ 999 の整数。デフォルトは 10 です。

ステップ 3　新しいユーザ フィルタを追加します。次のコマンドを入力します。

```
user-filter row-num filter-action src-ip [ip-mask] protocol dest-port
[fragments-type] [rate-limit rate burst units]
```

表 7-13 に、**user-filter** コマンドの引数を示します。

表 7-13　user-filter コマンドの引数とキーワード

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号。行番号はフィルタの ID で、これによって複数のユーザ フィルタの優先順位が定義されます。Guard モジュールは、行番号の昇順でフィルタを操作します。
filter-action	特定のトラフィック タイプに対してフィルタが実行するアクションを指定します。詳細については、表 7-11 を参照してください。
フローの引数とキーワード	フィルタリングを実行する対象のフロー。*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 7-1 を参照してください。
rate	レートの制限を指定する 64 より大きい整数。ユーザ フィルタは、トラフィックをこのレートに制限します。単位は、*units* パラメータで指定されます。デフォルトでは、フィルタのトラフィック レートは制限されません。*rate* リミットは、最大で *burst* リミットの 10 倍まで指定可能です。
burst	トラフィックのバースト リミットを指定する 64 より大きい整数。単位は、*units* パラメータで指定される単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。*burst* リミットは、最大で *rate* リミットの 8 倍まで指定可能です。
units	レート リミットの単位。次の単位を指定できます。 • **bps**：ビット / 秒 • **kbps**：キロビット / 秒 • **kpps**：キロパケット / 秒 • **mbps**：メガビット / 秒 • **pps**：パケット / 秒

次の例は、ユーザ フィルタの番号を 10 から開始してそれぞれ 5 ずつ変更し、行番号 *12* にユーザ フィルタを追加する方法を示しています。このフィルタは、プロトコルが *6*（TCP）で宛先ポート *25*（SMTP）に向かうすべての送信元 IP アドレスからのトラフィックを対象とします。また、このフィルタでは、特定のフローは許可されますが、フロー レートは *600 pps* に、バースト サイズは *400* パケットにそれぞれ制限されています。

```
user@GUARD-conf-zone-scannet# user-filter renumber 10 5
user@GUARD-conf-zone-scannet# user-filter 12 permit * 6 25 rate-limit 600 400 pps
```

ユーザ フィルタの表示

ユーザ フィルタは、ゾーンの設定の一部です。ユーザ フィルタを表示するには、ゾーンのプロンプトで、**show** コマンドまたは **show running-config** コマンドを使用します。

ヒント　ユーザ フィルタの設定をディスプレイの先頭に表示するには、**show** コマンドまたは **show running-config** コマンドを **| begin USER FILTERS** オプションを指定して使用します。

表 7-14 に、**show** コマンドの出力におけるユーザ フィルタのフィールドを説明します。

表 7-14　show コマンドにおけるユーザ フィルタのフィールドの説明

フィールド	説明
Row	ユーザ フィルタの優先順位を示します。
Filter flow	フィルタリングを実行する対象のフローを示します。Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 7-2 を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィック レートを pps で示します。

表 7-14　show コマンドにおけるユーザ フィルタのフィールドの説明（続き）

フィールド	説明
Action	フィルタが特定のトラフィック タイプに対して実行するアクションを示します。詳細については、表 7-11 を参照してください。
Rate	ユーザ フィルタで処理可能なトラフィック レートの制限を示します。レートは、*Units* フィールドで指定された単位で表示されます。
Burst	フィルタで特定のフローに対して許可されるトラフィックのバースト リミットを示します。単位は、*Units* フィールドで指定されるレートの単位に応じて、ビット、キロビット、キロパケット、メガビット、またはパケットになります。
Units	レートとバースト レートが表示される単位を示します。

ユーザ フィルタの削除

ユーザ フィルタを削除するには、次の手順を実行します。

ステップ 1　ユーザ フィルタのリストを表示し、削除するユーザ フィルタの行番号を確認します。詳細については、前の項、「ユーザ フィルタの表示」を参照してください。

ステップ 2　フィルタを削除します。次のコマンドを入力します。

```
no user-filter row-num
```

row-num 引数には、ユーザ フィルタの行番号を指定します。すべてのユーザ フィルタを削除するには、* を入力します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# no user-filter *
```

注意　すべてのユーザ フィルタを削除する場合、ポリシーのアクションが to-user-filter（ポリシーのアクションの詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照）に設定されているときには、保護されていないトラフィックがゾーンに渡されます。

動的フィルタの設定

Guard は、トラフィック フローを分析した結果として動的フィルタを作成します。このフィルタは、特定のトラフィック フローを関連する保護モジュールに誘導します。この一連のフィルタは Guard モジュールによって、ゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整されます。動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。

Guard は、トラフィックの異常を検出する中で、ゾーンが宛先になっているトラフィックを継続的に分析します。フローがポリシーのしきい値を超過すると、異常が発見されます。異常なトラフィック パターンを検出すると、攻撃の処理方法を定義する動的フィルタの作成を開始します。

Guard モジュールは、すべてのトラフィックをユーザ フィルタに誘導する最初の動的フィルタを追加します。Guard モジュールが十分な時間をかけて攻撃を分析するまでの間、ユーザ フィルタは新たに発生する DDoS 攻撃に対して最初の防御策を提供します。

Guard モジュールはユーザ フィルタと動的フィルタの両方を調べた後で、当該トラフィック フローの処理方法を決定します。コンパレータは、フローに一致する最初のユーザ フィルタを動的フィルタと比較し、提案された中で最も強力な保護措置を選択します。そして、認証のためにトラフィックを関連する保護モジュールに誘導します。動的フィルタまたはユーザ フィルタが実行するアクションは、重大度レベルの大きい順に、drop、strong、basic、permit です。アクション redirect/zombie および block-unauthenticated が指定された動的フィルタは、同じタイプのトラフィックを処理するユーザ フィルタがあっても適用されます。動的フィルタは Guard モジュールの認証メカニズムに影響しますが、トラフィック フローには直接影響を及ぼさないためです。

動的フィルタにアクセスし、独自のニーズに合うように設定することができます。

表 7-15 に、動的フィルタで実行可能なさまざまなアクションを説明します。

表 7-15　動的フィルタのアクション

アクション	説明
drop	トラフィックをドロップします。
strong	特定のトラフィックにスプーフィング防止の強化保護メカニズムを適用します。
to-user-filters	ユーザ フィルタにトラフィックを転送します。デフォルトのユーザ フィルタを変更した場合は、これらの動的フィルタを処理するユーザ フィルタが存在することを確認してください。
block-unauthenticated-basic	基本的なスプーフィング防止メカニズムを機能拡張したもので、認証されなかったトラフィック フローをドロップします。
block-unauthenticated-strong	強力なスプーフィング防止メカニズムを機能拡張したもので、認証されなかったトラフィック フローをドロップします。
block-unauthenticated-dns	DNS のスプーフィング防止メカニズムで非認証と定義された、DNS UDP サーバに向かうトラフィック フロー（プロトコルが UDP、ポートが 53 のもの）をドロップします。
redirect/zombie	**basic/redirect** のアクションが指定されたすべてのユーザ フィルタの認証を強化します。

動的フィルタは、アクティブな状態が一定時間持続するよう設定されています。動的フィルタのタイムアウトに関するパラメータは、フィルタがどのように作成されたかによって、次のいずれかの方法で設定されます。

- ゾーン　ポリシーによって作成された動的フィルタ：動的フィルタのタイムアウトは、ポリシーのタイムアウトに設定されています。ポリシーによって作成される追加の動的フィルタのタイムアウトを変更するには、動的フィルタが生成される原因となったポリシーのタイムアウトを変更します。ポリシー設定モードで **timeout** コマンドを使用します。
- ユーザ定義の動的フィルタ：動的フィルタのタイムアウトは、**dynamic-filter** コマンドの *exp-time* 引数を使用して定義します。

動的フィルタのタイムアウト期限が満了すると、Guard は、現在のトラフィックの状態に基づいて動的フィルタを非アクティブにするかどうかを判断します。Guard が動的フィルタを非アクティブにしないと決定した場合、フィルタはさらにある期間アクティブのままになります。詳細については、P.7-38 の「動的フィルタの非アクティブ化」を参照してください。

動的フィルタを追加または削除し、ニーズに合せて設定することができます。動的フィルタは、Guard モジュールによって現在保護されているゾーンに対してだけ追加することができます。Guard モジュールは、ゾーンの保護が終了すると、動的フィルタを消去します。

この項では、次のトピックについて取り上げます。

- 動的フィルタの追加
- 動的フィルタの表示
- 動的フィルタの削除
- 動的フィルタの非アクティブ化

動的フィルタの追加

動的フィルタを追加するには、次のコマンドを入力します。

dynamic-filter *action* {***exp-time*** | **forever**} ***src-ip*** [***ip-mask***] ***protocol dest-port*** [***fragments-type***]

複数の動的フィルタを追加するには、**dynamic-filter** コマンドを複数使用します。

表 7-16 に、**dynamic-filter** コマンドの引数を示します。

表 7-16　dynamic-filter コマンドの引数とキーワード

パラメータ	説明
action	フィルタが特定のトラフィック フローに対して実行するアクション。詳細については、表 7-15 を参照してください。
exp-time	フィルタがアクティブである期間（秒単位）を指定する、1 ～ 3,000,000 の整数。

表 7-16　dynamic-filter コマンドの引数とキーワード（続き）

パラメータ	説明
forever	フィルタは無限にアクティブです。保護が終了すると、フィルタは削除されます。
フローの引数とキーワード	フィルタリングを実行する対象のフロー。*src-ip*、*ip-mask*、*protocol*、*dest-port*、および *fragments-type* の詳細については、表 7-1 を参照してください。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# dynamic-filter to-user-filters 600
192.128.30.45 255.255.255.252 6 88 no-fragments
```

動的フィルタの表示

Guard モジュールによって作成された動的フィルタを表示するには、**show dynamic-filters** コマンドを使用します。このコマンドには、次のオプションが用意されています。

- **show dynamic-filters** [details]：すべての動的フィルタのリストを表示します。
- **show dynamic-filters** *dynamic-filter-id* [details]：特定の動的フィルタを 1 つ表示します。
- **show dynamic-filters sort** {action | exp-time | id | filter-rate}：すべての動的フィルタのソートされたリストを表示します。

（注） 保留動的フィルタを表示するには、**show recommendations** コマンドを使用します。詳細については、第 9 章「インタラクティブ保護モード」を参照してください。

表 7-17 に、**show dynamic-filters** コマンドの引数を示します。

表 7-17　show dynamic-filters コマンドの引数

パラメータ	説明
dynamic-filter-id	表示する特定の動的フィルタの識別番号（ID）。この整数は Guard モジュールによって割り当てられます。フィルタの ID を確認するには、すべての動的フィルタのリストを表示します。
details	動的フィルタの詳細情報を表示します。詳細情報には、攻撃フローに関する追加情報、トリガーとなるレート、およびそのフィルタを作成したポリシーなどがあります。
action	厳密度の最も高いもの（ドロップ）から低いもの（通知）まで、動的フィルタをアクション別に表示します。
exp-time	動的フィルタを有効期限の昇順で表示します。
id	動的フィルタを ID 番号の昇順で表示します。
filter-rate	動的フィルタをトリガーとなるレート（pps）の昇順で表示します。

（注） Guard モジュールは、最大 1,000 個の動的フィルタを表示します。1,000 を超える動的フィルタがアクティブになっている場合は、ログ ファイルまたはゾーンのレポートで、動的フィルタに関するすべてのリストを確認してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show dynamic-filters 876 details
```

表 7-18 に、**show dynamic-filters** コマンドの出力フィールドを説明します。

表 7-18　show dynamic-filters コマンド出力のフィールドの説明

フィールド	説明
ID	フィルタの識別番号を示します。
Action	フィルタがトラフィック フローに対して実行するアクションを示します。詳細については、表 7-15 を参照してください。
Exp Time	フィルタがアクティブになっている時間を示します。この時間が経過すると、フィルタは **filter-termination** コマンドを使用して定義済みのしきい値に従って削除される場合があります。
Filter flow	フィルタリングを実行する対象のフローを示します。Source IP、Source Mask、Proto、DPort、Frg の詳細については、表 7-2 を参照してください。
RxRate (pps)	このフィルタについて測定されている現在のトラフィック レートを pps で示します。

表 7-19 に、**show dynamic-filters details** コマンドの追加の出力フィールドを説明します。

表 7-19　show dynamic-filters details コマンドのフィールドの説明

フィールド	説明
Attack flow	軽減が図られた攻撃フローの特性を示します。Dynamic Filters テーブルに表示される軽減が図られた攻撃フローの範囲は、攻撃フローの範囲より広い場合があります。たとえば、ポート 80 に対するスプーフィングを利用しない攻撃では、ポート 80 からのトラフィックだけではなく、該当する送信元 IP アドレスからのすべての TCP トラフィックがブロックされます。フロー フィールドの詳細については、表 7-2 を参照してください。
Triggering Rate	ポリシーのしきい値を超過した攻撃フローのレートを示します。

表 7-19　show dynamic-filters details コマンドのフィールドの説明（続き）

フィールド	説明
Threshold	攻撃フローによって超過したポリシーのしきい値を示します。
Policy	特定の動的フィルタを作成したポリシーを示します。詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください。

動的フィルタの削除

動的フィルタを削除することができます。ただし、削除が有効になる期間は限られています。Guard モジュールは、ゾーンが保護されている限り、継続的に新しい動的フィルタを設定するためです。

動的フィルタを削除するには、次の手順を実行します。

ステップ 1　動的フィルタのリストを表示し、削除する動的フィルタの ID を確認します。詳細については、前の項、「動的フィルタの表示」を参照してください。

ステップ 2　関連する動的フィルタを削除します。次のコマンドを入力します。

no dynamic-filter *dynamic-filter-id*

dynamic-filter-id 引数には、動的フィルタの ID を指定します。すべての動的フィルタを削除するには、アスタリスク（*）を入力します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# no dynamic-filter 876
```

必要のない動的フィルタが再作成されないようにするには、次のいずれかのアクションを実行します。

- 動的フィルタを作成するポリシーを非アクティブにします（詳細については、P.8-22 の「ポリシーの状態の変更」を参照）。不要な動的フィルタを作成したポリシーを発見するには、P.7-34 の「動的フィルタの表示」を参照してください。
- 目的のトラフィック フロー用のバイパス フィルタを設定します（詳細については、P.7-21 の「バイパス フィルタの設定」を参照）。
- 不要な動的フィルタを作成したポリシーのしきい値を大きくします（詳細については、P.8-23 の「ポリシーのしきい値の設定」を参照）。

動的フィルタの非アクティブ化

動的フィルタのタイムアウト期限が満了すると、Guard は、現在のトラフィックの状態に基づいて動的フィルタを非アクティブにするかどうかを判断します。Guard が動的フィルタを非アクティブにしないと決定した場合、フィルタはさらにある期間アクティブのままになります。

動的フィルタは、次のいずれか 1 つの条件に当てはまる場合に非アクティブになります。

- ゾーンの悪意のあるトラフィック　レートの合計（スプーフィングされたトラフィックとドロップされたトラフィックの合計と等しい）が、zone-malicious-rate 終了しきい値以下である（この項で次に示すコマンドを参照）。
- 動的フィルタでトラフィック レートが測定され（フィルタのレート カウンタに N/A と表示されていない）、**かつ** filter-rate 終了しきい値（この項で次に示すコマンドを参照）が次の**両方**の値以上である。
  - 動的フィルタの現在のトラフィック レート
  - ユーザが設定した期間内の動的フィルタの平均トラフィック　レートこの期間は、ポリシーのタイムアウト パラメータで定義されます。詳細については、P.8-30 の「ポリシーのタイムアウトの設定」を参照してください。

（注） アクション to-user-filters、block-unauthenticated、redirect/zombie、または notify が指定された動的フィルタでは、トラフィック レートは測定されません。

ゾーンの悪意のあるトラフィックのしきい値を設定するには、次のコマンドを入力します。

filter-termination zone-malicious-rate *threshold*

threshold 引数には、ゾーンの悪意のあるトラフィックのしきい値を pps 単位で指定します。このトラフィックは、スプーフィングされたトラフィックとドロップされたトラフィックの合計で構成されます。デフォルト値は 50 pps です。

動的フィルタのレート終了しきい値を設定するには、次のコマンドを入力します。

filter-termination filter-rate *threshold*

threshold 引数には、動的フィルタのトラフィックのしきい値を pps 単位で指定します。デフォルト値は 2 pps です。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# filter-termination zone-malicious-rate 200
user@GUARD-conf-zone-scannet# filter-termination filter-rate 50
```

CHAPTER 8

ポリシー テンプレートとポリシーの設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）のポリシー、ポリシー構造、およびポリシー テンプレートについて説明します。また、ポリシーとポリシー テンプレート パラメータの設定方法を示します。

この章には、次の項があります。

- ポリシーについて
- ポリシー テンプレートについて
- ポリシー パスのセクションについて
- ポリシー パラメータの設定
- ポリシーの監視
- スナップショットを使用したラーニング プロセスの結果の確認

ポリシーについて

トラフィック フローの統計分析を行うために、Guard は、特定のトラフィック タイプの処理に関する定義を持っています。これらの定義をポリシーといいます。ポリシーは、Guard モジュール統計エンジンの構成要素です。各ゾーンには、ゾーンのトラフィック パターンに合せて調整されたポリシーのセットがあります。これらのポリシーは、悪意となる可能性のある異常をトレースするために、Guard モジュールがゾーンのトラフィックと比較する基礎となります。ポリシーは、トラフィック フローを持続的に測定し、特定のトラフィック フローが悪意のあるものまたは異常であると判断すると、そのフローに対してアクションを実行します。このアクションは、フローがポリシーのしきい値を超過すると発生します。

ゾーンの特定のトラフィック特性に合ったポリシーを作成するために、Guard モジュールは 2 つのフェーズのラーニング プロセスでゾーンのトラフィックをラーニングします。Guard モジュールは、定義済みのポリシー テンプレートを使用してポリシーを構築します。各ポリシー テンプレートは、ポリシーの作成に使用され、特定の DDoS 脅威に対する保護のために Guard モジュールが必要とする保護面を扱います。

ポリシーの作成後、ポリシーの追加および削除、またはポリシー パラメータの変更を行うことができます。

ポリシー パス構造

Guard モジュールは、ゾーンのトラフィック フローに関する統計分析を行います。各ポリシーは、特定のトラフィック フローを測定します。ポリシーは、Guard モジュールが分析に使用する特性を定義します。ポリシー名はセクションで構成されます。各セクションは、異なるトラフィック特性に関連する異なる役割を示します。たとえば、ポリシー *http/80/analysis/syns/src_ip* は、Guard モジュールの分析保護モジュールによって認証され、送信元 IP アドレスに応じて集約された、ポート 80 宛ての HTTP SYN パケットのトラフィック フローを測定します。

図 8-1 に、ポリシー名の例を示します。

図 8-1　　ポリシー名

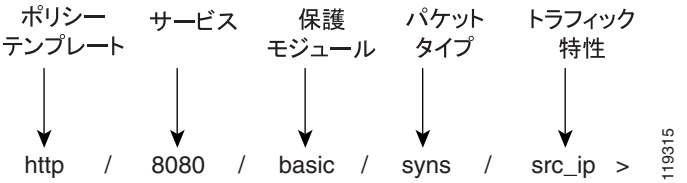


表 8-1 で、ポリシー名のセクションについて詳しく説明します。

表 8-1　　ポリシー名のセクション

セクション	説明
ポリシー テンプレート	ポリシーの構築に使用されたポリシー テンプレートを示します。各ポリシー テンプレートは、特定の DDos 脅威に対する保護のために Guard モジュールが必要とする保護面を扱います。詳細については、P.8-5 の「ポリシー テンプレートについて」を参照してください。
サービス	保護ポリシーに関連するポート番号またはプロトコル番号を示します。詳細については、P.8-14 の「サービス」を参照してください。
保護モジュール	Guard モジュールがトラフィック フローの処理に使用する保護モジュールを示します。詳細については、P.8-18 の「保護モジュール」を参照してください。
パケット タイプ	Guard モジュールが監視するパケット タイプを示します。詳細については、P.8-18 の「パケット タイプ」を参照してください。
トラフィック特性	Guard モジュールがポリシーの集約に使用するトラフィック特性を示します。詳細については、P.8-20 の「トラフィック特性」を参照してください。

ポリシー名の最初の 4 つのセクション（ポリシー テンプレート、サービス、保護モジュール、および パケット タイプ）では、分析するトラフィックのタイプが定義されます。ポリシー パスの最後のセクション（トラフィック特性）では、フローの分析方法が定義されます。

ポリシーには、相互依存性および優先度があります。同じトラフィック フローを定義する 2 つのポリシーがある場合、Guard モジュールは、より限定的なポリシーを使用してフローを分析します。たとえば、TCP サービスに関連するポリシーでは、HTTP 関連のポリシーによって処理される HTTP サービスが除外されます。

ポリシーの動作面を設定できます。動作面では、何がポリシーをトリガーするか、およびポリシーがアクティブになったときにポリシーが実行するアクションが定義されます。詳細については、P.8-21 の「ポリシー パラメータの設定」を参照してください。

ポリシーの作成

Guard モジュールは、ラーニング プロセスでゾーンのポリシーを作成します。ラーニング プロセスは次の 2 つのフェーズで構成されます。これらのフェーズで Guard はゾーンのトラフィックをラーニングし、特定のゾーン トラフィックの特性に対応します。

1. **ポリシー構築フェーズ**：このフェーズでは、Guard はポリシー テンプレートを使用してゾーンのポリシーを構築します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービスを検出できます。
2. **しきい値調整フェーズ**：このフェーズでは、Guard はゾーンのサービスのトラフィック レートに合せてポリシーしきい値を調整します。トラフィックが透過的に Guard を通過し、Guard はポリシー構築フェーズ中に検出されたサービスのしきい値を調整できます。

詳細については、P.6-13 の「ゾーン トラフィックの特性のラーニング」を参照してください。

ポリシー テンプレートについて

ポリシー テンプレートは、ポリシー構築の規則をまとめたものです。Guard モジュールは、ポリシー構築フェーズでポリシー テンプレートを使用し、ゾーンのポリシーを作成します。ポリシー構築フェーズの終わりの各テンプレートの出力は、ポリシーのグループです。ポリシー テンプレートの名前は、作成されるすべてのポリシーに共通の特性に由来しています。テンプレートの名前として、プロトコル（DNS など）、アプリケーション（HTTP など）、または目的（ip_scan など）が使用されます。たとえば、ポリシー テンプレート *tcp_connections* は、同時接続数など、接続に関連するポリシーを生成します。新しいゾーンを作成するときに、Guard モジュールによって一連のポリシー テンプレートがゾーン設定に組み込まれます。

表 8-2 で、Guard モジュールのポリシー テンプレートについて説明します。GUARD_DEFAULT ゾーン テンプレートを使用して新しいゾーンを作成するときに、Guard モジュールによってこれらのポリシー テンプレートが組み込まれます。

表 8-2　ポリシー テンプレート

ポリシー テンプレート	構築される一連のポリシーの関連先
dns_tcp	DNS-TCP プロトコル トラフィック。
dns_udp	DNS-UDP プロトコル トラフィック。
fragments	断片化されたトラフィック。
http	ポート 80（デフォルト）または他のユーザ設定ポートを経由する HTTP トラフィック。

表 8-2　ポリシー テンプレート（続き）

ポリシー テンプレート	構築される一連のポリシーの関連先
ip_scan	IP スキャニング（1 つのクライアントが特定の送信元 IP アドレスからゾーン内の多数の宛先 IP アドレスにアクセスしようとする状況）。このポリシー テンプレートは、定義されたゾーンがサブネットである場合に適しています。 デフォルトでは、このポリシー テンプレートはディセーブルになっています。このポリシー テンプレートのデフォルト アクションは、*notify* です。 **（注）** このポリシー テンプレートから生成されたポリシーはリソース消費量が多いため、パフォーマンスに影響を及ぼす可能性があります。
other_protocols	TCP および UDP 以外のプロトコル。
port_scan	ポート スキャニング（1 つのクライアントが特定の送信元 IP アドレスからゾーン内の多数のポートにアクセスしようとする状況）。 デフォルトでは、このポリシー テンプレートはディセーブルになっています。このポリシー テンプレートのデフォルト アクションは、*notify* です。 **（注）** このポリシー テンプレートから生成されたポリシーはリソース消費量が多いため、パフォーマンスに影響を及ぼす可能性があります。
tcp_connections	TCP 接続の特性。
tcp_not_auth	Guard のスプーフィング防止メカニズムによって認証されていない TCP 接続。
tcp_outgoing	ゾーンによって開始された TCP 接続。

表 8-2　ポリシー テンプレート（続き）

ポリシー テンプレート	構築される一連のポリシーの関連先
tcp_ratio	異なるタイプの TCP パケット間の比率。たとえば、SYN パケットと FIN/RST パケットの比率に関連するものです。
tcp_services	HTTP 関連のポート（ポート 80 やポート 8080 など）以外のポート上の TCP サービス。
tcp_services_ns	TCP サービス。デフォルトでは、このポリシー テンプレートから作成されるポリシーは、IRC ポート（666X）、SSH、および Telnet に関連するものになります。このポリシー テンプレートは、Guard モジュールで強化保護メカニズムを使用することが必要なアクションを持つポリシーを作成しません。
udp_services	UDP サービス。

（注） Guard は、まず専用ポート 6660 ～ 6670 および 21 ～ 23 上の TCP トラフィックのインジケータになります。

- これらのポート上でトラフィックがトレースされる場合、tcp_services_ns ポリシー テンプレートがポリシー グループを構築し、tcp_services ポリシー テンプレートが他のポート上の TCP サービスを担当します。
- これらのポート上でトラフィックがトレースされない場合、tcp_services_ns ポリシー テンプレートは動作しません。

tcp_services_ns ポリシー テンプレートから作成されたポリシーにはサービスを追加できます。

Guard には、TCP プロキシのスプーフィング防止メカニズムを使用しないゾーンを保護するための追加のポリシー テンプレートが用意されています。ゾーンが IP アドレスに応じて管理される場合（Internet Relay Chat（IRC; インターネット リレー チャット）サーバタイプ ゾーンなど）、またはゾーンでどのようなタイプのサービスが実行されているか分からない場合は、このようなポリシー テンプレートを使用できます。

GUARD_TCP_NO_PROXY ゾーン テンプレートでゾーンを定義する場合、Guard モジュールによって、表 8-3 に示されるポリシー テンプレートが使用されます。Guard モジュールは、http、tcp_connections、および tcp_outgoing のポリシー テンプレートをそれぞれ http_ns、tcp_connections_ns、および tcp_outgoing_ns のポリシー テンプレートに置き換えます。http_ns、tcp_connections_ns、および tcp_outgoing_ns のポリシー テンプレートは、Guard モジュールで強化保護メカニズムを使用することが必要なアクションを持つポリシーを作成しません。

表 8-3 に、GUARD_TCP_NO_PROXY の Guard ポリシーを詳細に説明します。

表 8-3　GUARD_TCP_NO_PROXY のポリシー テンプレート

ポリシー テンプレート	構築される一連のポリシーの関連先
tcp_connections_ns	TCP 接続の特性。
tcp_outgoing_ns	ゾーンによって開始された TCP 接続。
http_ns	ポート 80（デフォルト）または他のユーザ設定ポートを経由する HTTP トラフィック。

すべてのポリシー テンプレートのリストを表示するには、ゾーン設定モードで **policy-template** コマンドを入力し、Tab キーを 2 回押してください。

ポリシー テンプレート パラメータの設定

ラーニング プロセス中、ゾーンのトラフィックは Guard を透過的に通過します。アクティブな各ポリシー テンプレートは、ゾーンのトラフィックの特性に応じてポリシーのグループを生成します。Guard では、特定のポリシー テンプレートから Guard が生成するポリシーの最大数を定義できます。Guard は、ポリシー テンプレートに関連するサービスをトラフィック量のレベルによってランク付けします。次に Guard は、定義済みの最小しきい値を超過したサービスの中で最大のトラフィック量を持つサービスをピックアップして、各サービスのポリシーを作成します。一部のポリシー テンプレートは、特定のポリシーが追加されていないすべてのトラフィック フローを処理するために、追加のポリシーを作成します。このようなポリシーは、*any* というサービスで追加されます。

次のポリシー テンプレート パラメータを設定できます。

- サービスの最大数の設定：Guard がポリシー テンプレートから特定のポリシーを作成するときの対象となるサービスの最大数を定義します。
- 最小しきい値の設定：Guard モジュールでサービスをランク付けするために超える必要のある最小しきい値を定義します。
- ポリシー テンプレートの状態の設定：Guard モジュールがポリシー テンプレートからポリシーを生成するかどうかを定義します。

ポリシー テンプレート パラメータを設定するには、ポリシー テンプレート設定モードに入ります。次のコマンドを入力します。

policy-template *policy-template-name*

policy-template-name 引数には、ポリシー テンプレートの名前を指定します。詳細については、表 8-2 を参照してください。

このコマンドを実行すると、Guard モジュールはポリシー テンプレート設定モードに入ります。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# policy-template http
user@GUARD-conf-zone-scannet-policy_template-http#
```

特定のポリシー テンプレートのパラメータを表示するには、ポリシー テンプレート設定モードで **show** コマンドを使用します。

サービスの最大数の設定

サービスの最大数のパラメータは、ポリシー テンプレートがピックアップしてポリシーを作成する対象となるサービスの最大数（プロトコル番号やポート番号）を定義します。Guard は、ポリシー テンプレートに関連するサービスをトラフィック量のレベルによってランク付けします。Guard は、定義済みの最小しきい値（*min-threshold* パラメータで定義）を超過したサービスの中で最大のトラフィック量を持つサービスをピックアップして、各サービスのポリシーを作成します。そのポリシー テンプレートの特性を備えた他のすべてのトラフィック フローを処理する追加のポリシーが、*any* というサービスで追加されることがあります。

（注） サービスの最大数が大きいほど、ゾーンが使用するメモリが多くなります。

このパラメータは、サービスを検出するポリシー テンプレート（tcp_services、tcp_services_ns、udp_services、および other protocols など）にのみ定義できます。特定のサービスに関連するポリシー テンプレート（サービス 53 に関連する *dns_tcp* など）や特定のトラフィック特性に関連するポリシー テンプレート（*fragments* など）にこのパラメータを設定することはできません。

Guard は、ポリシーのトラフィック特性に基づいてサービスへのトラフィック レートを測定します。このトラフィック特性とは、送信元 IP アドレス、宛先 IP アドレス、または送信元ネットです。サービス *any* に関連するポリシーは、特定のポリシーによって処理されないすべてのサービスの送信元 IP アドレスのレートを測定します。したがって、こちらの値は精度が劣ります。

サービスの数を制限すると、希望のトラフィック フロー要件に合せて Guard のポリシーを設定できます。

サービスの最大数を設定するには、次のコマンドを入力します。

max-services *max-services*

max-services 引数は、Guard がピックアップするサービスの最大数を定義する、1 より大きい整数です。サービスの最大数が 10 を超えないようにすることをお勧めします。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# max-services 5
```

最小しきい値の設定

最小しきい値のパラメータは、サービスの最小トラフィック量を定義します。このしきい値を超過すると、Guard は、しきい値を超過した特定のトラフィック フローに応じて、サービスのトラフィックに関連するポリシーを構築します。

このパラメータは、正しいゾーン保護に不可欠であるためにポリシーを常に構築するポリシー テンプレート（tcp_services、tcp_services_ns、udp_services、other_protocols、http、および fragments）には設定できません。

このしきい値を設定すると、Guard の保護をゾーンのサービスのトラフィック量に、よりよく適合させることができます。

最小しきい値を設定するには、次のコマンドを入力します。

min-threshold *min-threshold*

min-threshold 引数は、0 以上の実数（小数点以下が 2 桁の浮動小数点型の数字）で、最小しきい値レート（pps）を定義します。同時接続および SYN/FIN の比率を測定する場合、しきい値は接続の合計数を定義する整数になります。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet-policy_template-http# min-threshold 12.3
```

ポリシー テンプレートの状態の設定

このパラメータは、ポリシー テンプレートの状態を定義します。ポリシー テンプレートは、イネーブルまたはディセーブルにすることができます。ポリシー テンプレートをディセーブルにすると、Guard がポリシー構築フェーズを経ても、ポリシー テンプレートからポリシーが生成されません。

注意　ポリシー テンプレートをディセーブルにすると、Guard はそのポリシー テンプレートに関連するトラフィックの種類からゾーンを保護できません。このため、保護の実効性が大幅に低下する可能性があります。たとえば、dns_udp ポリシー テンプレートをディセーブルにすると、Guard は DNS (UDP) 攻撃からゾーンを保護できなくなります。

ポリシー テンプレートをディセーブルにするには、**disable** コマンドを使用します。

ポリシー テンプレートをイネーブルにするには、**enable** コマンドを使用します。

すべてのポリシー テンプレート パラメータの同時設定

1 つのコマンドで、ポリシー テンプレートのすべての動作パラメータを設定できます。次のコマンドを入力します。

policy-template *policy-template-name max-services min-threshold* {**disabled** | **enabled**}

表 8-4 で、**policy-template** コマンドの引数とキーワードについて説明します。

表 8-4　policy-template コマンドの引数とキーワード

パラメータ	説明
policy-template-name	ポリシー テンプレート名。詳細については、表 8-1 を参照してください。
max-services	Guard がピックアップして特定のポリシー テンプレートからポリシーを構築する対象となるサービスの最大数。 Guard モジュールが現在の値を変更しないように防止するには、-1 を入力します。 詳細については、P.8-9 の「サービスの最大数の設定」を参照してください。
min-threshold	Guard モジュールでサービスをランク付けするために超える必要のある最小しきい値。 Guard モジュールが現在の値を変更しないように防止するには、-1 を入力します。 詳細については、P.8-11 の「最小しきい値の設定」を参照してください。

表 8-4　policy-template コマンドの引数とキーワード（続き）

パラメータ	説明
disabled	ポリシー テンプレートをディセーブルにして、ポリシーが生成されないようにします。詳細については、P.8-11 の「ポリシー テンプレートの状態の設定」を参照してください。
enabled	ポリシー テンプレートをイネーブルにします。詳細については、P.8-11 の「ポリシー テンプレートの状態の設定」を参照してください。

次の例は、ポリシー テンプレート *tcp_services* のパラメータを設定する方法を示しています。サービスの最大数は *3* に設定されます。最小しきい値は変更されず（*-1*）、ポリシーの状態は **enabled** に設定されます。

```
user@GUARD-conf-zone-scannet# policy-template tcp_services 3 -1 enabled
```

ポリシー パスのセクションについて

ポリシー パスは、次のセクションで構成されます。

- ポリシー テンプレート（ポリシー テンプレートについてを参照）
- サービス
- 保護モジュール
- パケット タイプ
- トラフィック特性

サービス

サービス セクションは、ポリシーに関連するゾーン アプリケーション ポートまたはプロトコルを示します。ポリシーには、相互依存性および優先度があります。同じトラフィック フローを定義する 2 つのポリシーがある場合、Guard モジュールは、より限定的なポリシーを使用してフローを分析します。サービス *any* は、同じポリシー テンプレートから作成された他のサービスと特に一致しないすべてのトラフィックに関連します。

ゾーンの主要サービスに対して最適に調整された保護が可能になるよう、特定のポリシーを定義することをお勧めします。

注意　複数のポリシーに同じサービス（ポート番号）を追加しないでください。

ゾーンのポリシーにサービスを追加または削除すると、Guard モジュールはゾーンのポリシーを未調整としてマークします。ゾーンが保護およびラーニング動作状態にある場合、次のいずれかの操作が実行されるまで、Guard モジュールはゾーン トラフィック内の異常を検出できません。

- ラーニング　プロセスのしきい値調整フェーズを実行して、その結果を受け入れる（P.6-19 の「しきい値の調整」を参照）。
- ゾーンのポリシーを調整済みとしてマークする（P.6-27 の「ポリシーへの調整済みのマーク付け」を参照）。

この項では、次のトピックについて取り上げます。

- サービスの追加
- サービスの削除

サービスの追加

特定のポリシー テンプレートから作成されたすべてのポリシーにサービスを追加できるので、より限定的なポリシーを作成できます。新しいサービスは、ポリシー構築フェーズ中に検出されたサービスに追加されます。新しいサービスは、デフォルト値を使用して定義されます。このしきい値は手動で定義することもできますが、しきい値調整フェーズを実行し（詳細については、P.6-19 の「しきい値の調整」を参照）、ポリシーをゾーンのトラフィックに合せて調整することをお勧めします。

新しいサービスを追加できるのは、次のポリシー テンプレートから作成されたポリシーです。

- tcp_services、udp_services、tcp_services_ns：サービスはポート番号を指定します。
- other_protocols：サービスはプロトコル番号を指定します。

（注） サービスの追加後にポリシー構築フェーズを実行すると、手動で追加したサービスを新しいサービスが上書きすることがあります。

次の状況において、ポリシー構築を再度実行しない場合は、サービスを手動で追加する必要があります。

- 新しいアプリケーションまたはサービスがゾーン　ネットワークに追加された。
- ポリシー構築フェーズの実行期間が短かったため、一部のネットワーク サービスが反映されていない（たとえば、週に 1 回のみあるいは夜間のみアクティブになる既知のアプリケーションまたはサービスがある）。

サービスを追加するには、ポリシー テンプレート設定モードで次のコマンドを入力します。

add-service *service-num*

または

ゾーン設定モードで次のコマンドを入力します。

policy-template *policy-template-name* **add-service** *service-num*

表 8-5 で、**policy-template** コマンドの引数について説明します。

表 8-5　policy-template コマンドの引数

パラメータ	説明
policy-template-name	ポリシー テンプレート名。詳細については、表 8-2 を参照してください。
service-num	プロトコル番号またはポート番号。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# add-service 25
```

サービスの削除

ポリシー テンプレートに関連する特定のサービスを削除できます。Guard モジュールは、特定のポリシー テンプレートで作成されたすべてのポリシーからサービスを削除します。

サービスを削除するには、ポリシー テンプレート設定モードで次のコマンドを入力します。

remove-service *service-num*

または

ゾーン設定モードで次のコマンドを入力します。

policy-template *policy-template-name* **remove-service** *service-num*

表 8-6 で、**remove-service** コマンドの引数について説明します。

表 8-6　remove-service コマンドの引数

パラメータ	説明
policy-template-name	ポリシー テンプレート名。詳細については、表 8-2 を参照してください。
service-num	削除するプロトコル番号またはポート番号。

注意　サービスを削除すると、Guard モジュールのポリシーがそのサービスのトラフィックに関連できなくなります。そのため、ゾーンの保護に支障をきたす恐れがあります。

次のポリシー テンプレートからサービスを削除できます。

- tcp_services、udp_services、tcp_services_ns：サービスはポート番号です。
- other_protocols：サービスはプロトコル番号です。

次の状況において、ラーニング プロセスのポリシー構築をアクティブにしない場合は、サービスを手動で削除する必要があります。

- アプリケーションまたはサービスがネットワークから削除された。
- イネーブルにするつもりのない（そのネットワーク環境では一般的でないため）アプリケーションまたはサービスが、ポリシー構築フェーズ中に識別された。

（注）　サービスの削除後にポリシー構築フェーズを実行すると、そのサービスが再度追加されることがあります。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# remove-service 25
```

保護モジュール

保護モジュール セクションは、Guard モジュールがトラフィック フローの処理に使用する保護モジュールを示します。このセクションは情報提供用で、保護モジュールを設定することはできません。Guard モジュールには、次の 3 つの保護モジュールがあります。

- **分析**: この保護モジュールでは、トラフィック フローが介入なしで流れます。
- **基本**：この保護モジュールでは、Guard モジュールの基本的なスプーフィング防止メカニズムが適用されます。Guard モジュールは、各ホストに対して認証を行います。認証は事前に定義された期間で有効です。この期間が経過すると、Guard モジュールはもう一度ホストを認証します。
- **強化**：この保護モジュールでは、Guard モジュールの強力なスプーフィング防止メカニズムが適用されます。Guard モジュールは、各接続に対して認証を行います。

メカニズムをアクティブにした後、Guard モジュールは引き続きトラフィックを分析します。Guard モジュールは、ゾーン宛てのトラフィックでトラフィック異常を検出すると、より強力な保護メカニズムをアクティブにします。

パケット タイプ

パケット タイプ セクションは、Guard モジュールが監視するパケット特性を示します。パケット特性は、次のいずれかです。

- パケット タイプ：たとえば、TCP-SYN パケット
- Guard モジュールによるパケット分析：たとえば、認証されたパケットや、接続が TCP ハンドシェイクを実行していることを Guard モジュールが確認したパケット。
- パケットの方向：たとえば、着信接続

表 8-7 で、Guard モジュールが監視するパケット タイプについて説明します。

表 8-7　パケット タイプ

パケット タイプ	簡単な説明
auth_pkts	TCP ハンドシェイクまたは UDP 認証を経たパケット。
auth_tcp_pkts	TCP ハンドシェイクを経たパケット。
auth_udp_pkts	UDP 認証を経たパケット。
in_nodata_conns	接続上でデータ転送のないゾーン着信接続（データ ペイロードのないパケット）。
in_conns	ゾーン着信接続。
in_pkts	ゾーンの着信 DNS クエリー パケット。
in_unauth_pkts	ゾーンの認証されていない着信 DNS クエリー。
num_sources	Guard のスプーフィング防止メカニズムによって認証された、ゾーン宛ての TCP 送信元 IP アドレスを持つパケットの数。
out_pkts	ゾーンの着信 DNS 応答パケット。
reqs	データ ペイロードを持つ要求パケット。
syns	同期パケット：TCP SYN フラグの付いたパケット。
syn_by_fin	SYN および FIN フラグの付いたパケット。Guard モジュールは SYN フラグの付いたパケット数と FIN フラグの付いたパケット数の比率を確認します。
unauth_pkts	TCP ハンドシェイクを経なかったパケット。
pkts	同じ保護レベルの他のどのカテゴリにも入らないすべてのパケット タイプ。

トラフィック特性

トラフィック特性セクションは、ポリシーの集約に使用されたトラフィック特性を示します。ポリシー名の最初の 4 つのセクション（ポリシー テンプレート、サービス、保護モジュール、および パケット タイプ）では、分析するトラフィックのタイプが定義されます。トラフィック特性では、トラフィック フローを分析する方法が定義されます。したがって、同じトラフィック フローを分析するが、異なる特性に応じてレートを測定する異なるポリシーが存在することがあります。たとえば、*dns_tcp/53/analysis/pkts/dst_ip* と *dns_tcp/53/analysis/pkts/src_ip* です。

表 8-8 で、Guard モジュールが監視するトラフィック特性について説明します。

表 8-8　トラフィック特性

トラフィック特性	簡単な説明
dst_ip	ゾーンの IP アドレス宛てのトラフィック。
dst_ip_ratio	特定の IP アドレス宛ての、SYN フラグの付いたパケットと FIN フラグの付いたパケットの比率。
dst_port	特定のゾーン ポート宛てのトラフィック。
dst_port_ratio	特定のポート宛ての、SYN フラグの付いたパケットと FIN フラグの付いたパケットの比率。
global	他のポリシー セクションによって定義されたすべてのトラフィック フローの合計。
protocol	プロトコルに応じて集約された、ゾーン宛てのトラフィック。
src_ip	送信元 IP アドレスに応じて集約された、ゾーン宛てのトラフィック。
src_ip_many_dst_ips	多数のゾーン IP アドレスが同じポートにあることを調査する 1 つの IP アドレスからのトラフィック。このキーは IP スキャニングに使用されます。
src_ip_many_ports	1 つのゾーン宛先 IP アドレスに多数のポートがあることを調査する 1 つの IP アドレスからのトラフィック。このキーはポート スキャニングに使用されます。

ポリシー パラメータの設定

ラーニング プロセスの完了後、特定のポリシー パラメータを表示できます。ポリシー パラメータを表示すると、ポリシー パラメータがゾーンのトラフィックに適しているかどうかを判断できます。1 つのポリシーまたはポリシーのグループを設定できます。必要に応じて、ポリシー パラメータを設定し、ポリシーをゾーンのトラフィック要件に適合させることができます。

ポリシー パラメータの設定を表示するには、ポリシー設定モードで **show** コマンドを使用します。

1 つの特定のポリシーまたはポリシーのグループを設定できます。

ポリシー設定モードに入るには、ゾーン設定モードで次のコマンドを入力します。

policy *policy-path*

policy-path 引数には、ポリシー パス セクションを指定します。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。

（注） ポリシー パス プロンプトで **policy ..** と入力すると、ポリシー パス階層で 1 レベル上に移動します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# policy dns_tcp/53/analysis/syns/global
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global#
```

次のパラメータを設定できます。

- ポリシーの状態：P.8-22 の「ポリシーの状態の変更」を参照してください。
- ポリシーのしきい値：P.8-23 の「ポリシーのしきい値の設定」を参照してください。
- ポリシーのタイムアウト：P.8-30 の「ポリシーのタイムアウトの設定」を参照してください。
- ポリシーのアクション：P.8-31 の「ポリシーのアクションの設定」を参照してください。

- ポリシーのインタラクティブ ステータス：P.8-32 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。

ポリシーのアクション、*タイムアウト*、*しきい値*、およびラーニング パラメータの引数は、ポリシー パスの各セクションで変更できます。ただし、高レベルのポリシー セクション（ポリシー テンプレート セクションやサービス セクションなど）でこれらのパラメータを変更すると、より多くのポリシーが影響を受けます。上位レベルのポリシー パス階層でこれらのパラメータを設定すると、すべてのサブポリシー パスでこれらのパラメータが変更されます。

Guard モジュールでは、**show policies** コマンドおよび **show policies statistics** コマンドを発行するときに、各ポリシー パス セクションでワイルドカード文字としてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しないと、指定していないセクションが Guard モジュールによってワイルドカード（*）と見なされます。
たとえば、ポリシーを *tcp_services//analysis//global* のように指定する場合です。

ポリシーの状態の変更

Guard モジュールのポリシーには、次の 3 つの状態があります。

- **Active**：ポリシーはトラフィックに関連付けられ、しきい値を超過した場合にアクションを実行します。
- **Inactive**：ポリシーはトラフィックに関連付けられ、しきい値を取得しますが、しきい値を超過してもアクションを実行しません。したがって、ポリシーが新しいしきい値調整ラーニング フェーズを経るようにする必要はありません。
- **Disabled**：ポリシーがトラフィック フローに関連付けられないため、しきい値が取得されません。このため、ポリシーに新しいしきい値調整フェーズを実行して、Guard モジュールでポリシーの正しいしきい値を監視する必要があります。

注意　ポリシーをディセーブルにすると、そのポリシーの対象となっていたトラフィックは、他のポリシーに属するものと見なされます。すべてのポリシーが新しいしきい値調整フェーズを経てから、ゾーン保護をアクティブにすることを強くお勧めします。

ポリシーの状態を変更するには、ポリシー設定モードで次のコマンドを入力します。

state {**active** | **disabled** | **inactive**}

次の例は、*/dns_tcp/53/analysis/syns* に一致するフローを持つすべてのポリシーの状態をディセーブルに設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns# state disabled
```

注意　ポリシーに対して不必要な非アクティブ化またはディセーブル化を行うと、Guard モジュールのポリシーが保護の役割を担わなくなり、ゾーンの保護に支障をきたす恐れがあります。

ポリシーをディセーブルにした後でポリシー構築フェーズを実行すると、トラフィック フローに応じてポリシーが再設定されます。その結果、ポリシーが再びアクティブになることがあります。

ポリシーのしきい値の設定

ポリシーのしきい値は、特定のポリシーのしきい値トラフィック レートを定義します。このしきい値を超過すると、ポリシーはゾーンを保護するアクションを実行します。しきい値は、デフォルトで、オンデマンド保護に適する値に設定されています。ポリシーのしきい値は、しきい値調整フェーズで調整されます。

しきい値は、次のポリシー テンプレートで構築されたポリシーを除き、pps で測定されます。

- **num_soruces**：しきい値は IP アドレスまたはポートの数で測定されます。
- **tcp_connections**：しきい値は接続の数で測定されます。
- **tcp_ratio**：しきい値は比率値で測定されます。

ポリシーのしきい値は、次の方法で設定できます。

- しきい値を設定する：ポリシーのしきい値を設定できます。P.8-24 の「ポリシーのしきい値の設定」を参照してください。

- しきい値を乗算する：Guard モジュールは現在のポリシーのしきい値に係数を掛けます。新しい値を固定値として設定しない場合、後続のしきい値調整フェーズでこの値が変更されることがあります。P.8-27 の「係数によるしきい値の乗算」を参照してください。
- 特定の IP しきい値を設定する：Guard モジュールはゾーンのアドレス範囲内にある特定の IP 送信元アドレスのしきい値を設定します。P.8-28 の「特定の IP しきい値の設定」を参照してください。
- **プロキシしきい値を設定する**：Guard モジュールは、プロキシを介して HTTP でゾーンに接続するクライアントのトラフィックのしきい値を設定します。P.8-29 の「プロキシしきい値の設定」を参照してください。

ポリシーのしきい値は、しきい値調整フェーズをさらに実行すると変更される場合があります。後続のしきい値調整フェーズでしきい値が変更されるかどうかは、次の方法で指定できます。

- **固定値としてしきい値を設定する**：Guard モジュールは後続のしきい値調整フェーズでポリシーのしきい値（proxy-threshold および threshold-list）を変更しません。P.8-25 の「固定値としてのしきい値の設定」を参照してください。
- **ポリシーのしきい値の固定乗数を設定する**：Guard モジュールは、現在のポリシーのしきい値、ラーニングしたしきい値、および固定乗数に基づいて、後続のしきい値調整フェーズでポリシーのしきい値を計算します。P.8-26 の「しきい値の乗数の設定」を参照してください。

ポリシーのしきい値の設定

ポリシーのしきい値を設定するには、次のコマンドを入力します。

threshold *threshold*

threshold 引数は、ポリシーのしきい値を指定する正数です。

次の例は、ポリシー policy dns_tcp/53/analysis/syns/global のしきい値を 300 に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global#
threshold 300
```

固定値としてのしきい値の設定

ポリシーのしきい値（proxy-threshold および threshold-list）を固定値として設定できます。Guard は、ラーニング プロセスのしきい値調整フェーズで新しいしきい値を無視し、現在の値を保持します。この機能により、ポリシーのしきい値を設定しながらも、引き続き他のポリシーのしきい値をラーニングすることが可能になります。

ポリシーのしきい値を固定値として設定するには、ポリシー設定モードで次のコマンドを入力します。

learning-params fixed-threshold

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global#
learning-params fixed-threshold
```

1 つのコマンドで、複数のポリシーのしきい値を固定値として設定できます。この場合、ゾーン設定モードでコマンドを使用します。ゾーン設定モードでポリシーのしきい値を固定値として設定するには、次のコマンドを入力します。

policy *policy-path* learning-params fixed-threshold

policy-path 引数には、ポリシー パスを指定します。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# policy dns_tcp learning-params fixed-threshold
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-parameters** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-parameters** コマンドを使用します。

しきい値の乗数の設定

ポリシーのしきい値の乗数を設定できます。Guard モジュールは、後続のしきい値調整フェーズの結果を受け入れる前に、ラーニングしたしきい値に指定の乗数を掛けてポリシーのしきい値を計算します。Guard モジュールは設定されたしきい値選択方式を使用して、しきい値調整フェーズの結果を受け入れます（P.6-26 の「しきい値選択方式の設定」を参照）。

ポリシーのしきい値の乗数を設定するには、ゾーン設定モードで次のコマンドを入力します。

policy ***policy-path*** **learning-params threshold-multiplier** *threshold-multiplier*

表 8-9 で、**learning-params threshold-multiplier** コマンドの引数について説明します。

表 8-9　learning-params threshold-multiplier コマンドの引数

パラメータ	説明
policy-path	乗数を掛ける対象のしきい値を持つポリシーのパス。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。
threshold-multiplier	ポリシーのしきい値に掛ける正の実数（小数点以下が 2 桁の浮動小数点型の数字）。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。

ポリシー設定モードでポリシーのしきい値の乗数を設定するには、**learning-params threshold-multiplier** *threshold-multiplier* コマンドを使用します。

次の例は、ポリシー テンプレート dns_tcp から作成されたポリシーのしきい値を半分にする方法を示しています。

```
user@GUARD-conf-zone-scannet# policy dns_tcp learning-params
threshold-multiplier 0.5
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-parameters** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-parameters** コマンドを使用します。

係数によるしきい値の乗算

1 つのポリシーまたはポリシーのグループのしきい値に係数を掛けることができます。このようにして、トラフィック量がゾーンのトラフィックを表さない場合に、1 つのポリシーまたはポリシーのグループのしきい値を増減できます。Guard モジュールは、ポリシーのしきい値、プロキシしきい値、および **policy threshold-list** コマンドを使用して定義されたしきい値を乗算します。

ポリシーのしきい値に係数を掛けるには、次のコマンドを入力します。

policy *policy-path* **thresh-mult** *threshold-multiply-factor*

表 8-10 で、**policy thresh-mult** コマンドの引数について説明します。

表 8-10　policy thresh-mult コマンドの引数

パラメータ	説明
policy-path	ポリシー テンプレート名。詳細については、表 8-2 を参照してください。
threshold-multiply-factor	しきい値に掛ける正の実数（小数点以下が 4 桁の浮動小数点型の数字）ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# policy */*/*/*/src_ip thresh-mult 0.5
```

しきい値は、Guard モジュールによって後続のしきい値調整フェーズで変更される場合があります。Guard モジュールによって、しきい値が後続のしきい値ラーニング フェーズで変更されないようにするには、しきい値を固定値として設定します。P.8-25 の「固定値としてのしきい値の設定」を参照してください。

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-parameters** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-parameters** コマンドを使用します。

特定の IP しきい値の設定

特定の IP しきい値を設定するには、次の方法を使用します。

- ある IP 送信元から大量のトラフィックがあることが分かっている場合は、特定の IP 送信元アドレスに適用するしきい値を設定できます。
- ゾーンの一部だけに宛てた大量のトラフィックがあることが分かっている非同種ゾーン（複数の IP アドレスが定義されているゾーン）の場合は、特定の IP 宛先アドレスに適用するしきい値を設定できます。

次のポリシーだけに、特定の IP しきい値を設定できます。

- トラフィック特性が宛先 IP（dst_ip）であるポリシー。
- デフォルト ポリシー アクションが drop である、トラフィック特性が送信元 IP（src_ip）アドレスのポリシー。デフォルト ポリシー アクションは、新しいゾーンを作成するときにポリシーが持っているアクションです。これらのポリシーには、ポリシー アクションを変更する場合でもしきい値のリストを設定できます。

特定の IP しきい値を設定するには、次のコマンドを入力します。

policy *policy-path* **threshold-list** *ip threshold* [*ip threshold ...*]

表 8-11 で、**policy threshold-list** コマンドの引数について説明します。

表 8-11　policy threshold-list コマンドの引数

パラメータ	説明
policy-path	ポリシー テンプレート名。詳細については、表 8-2 を参照してください。
ip	特定の IP アドレス。
threshold	しきい値トラフィック レート（pps）。ただし、同時接続および SYN 対 FIN の比率を測定するポリシーの場合、しきい値は接続数になります。

ポリシーごとに特定の IP しきい値を 10 個まで追加できます。特定の IP しきい値をすべて 1 つのコマンドで入力できます。

しきい値選択方式が new-thresholds に設定されている場合、Guard モジュールによって、ポリシーのしきい値が後続のしきい値調整フェーズで変更される場合があります（P.6-26 の「しきい値選択方式の設定」を参照）。

次の例は、ポリシー *http/80/analysis/syns/src_ip* に、IP アドレス *10.10.10.2* および *10.10.15.2* の特定の IP しきい値を設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip#
threshold-list 10.10.10.2 500 10.10.15.2 500
```

プロキシしきい値の設定

プロキシしきい値パラメータは、プロキシを介して HTTP でゾーンに接続するクライアントのトラフィック レートを定義します。プロキシしきい値により、Guard モジュールおよびユーザは、ポリシーをさまざまな送信元からのトラフィック量に適合させることができます。Guard モジュールはトラフィックをブロックするためだけにプロキシしきい値を使用します。したがってユーザは、強化保護モジュールを持つ、DEFAULT ゾーン テンプレート内のポリシー、および基本保護モジュールを持つ、TCP_NO_PROXY ゾーン テンプレート内のポリシーだけにプロキシしきい値を設定できます。

プロキシしきい値は、http、http_ns、tcp_connections、および tcp_connections_ns のポリシーだけに使用できます。ゾーンにアクティブな http または http_ns ポリシーがある場合にだけ、tcp_connections または tcp_connections_ns ポリシー テンプレートから作成されたポリシーのプロキシしきい値が有効になります。

プロキシしきい値を設定するには、次のコマンドを入力します。

proxy-threshold *proxy-threshold*

proxy-threshold 引数には、http ポリシーおよび http_ns ポリシーのプロキシしきい値のトラフィック レート（pps）を指定します。この引数は、tcp_connections ポリシーおよび tcp_connections_ns ポリシーの接続数でプロキシしきい値を指定します。

通常、プロキシ サーバが処理するトラフィック量はゾーンの一部であるネットワーク クライアントの処理量より多いため、プロキシしきい値を設定するときは、*proxy-threshold* 引数に *threshold* 引数より大きな値を設定することをお勧めします。

次の例は、ポリシー *tcp_ratio/any/basic/syn_by_fin/dst_ip_ratio* のプロキシしきい値を *20* に設定する方法を示しています。

```
user@GUARD-conf-zone-scannet-policy-/tcp_ratio/any/basic/syn_by_fin/
dst_ip_ratio# proxy-threshold 20
```

ポリシーのタイムアウトの設定

ポリシーによって生成される動的フィルタがそのアクションを適用する最小期間を定義するタイムアウト パラメータ。

タイムアウト期限が満了すると、Guard はプロシージャを実行して、ポリシーによって生成された動的フィルタを非アクティブにするかどうかを決定します。Guard が動的フィルタを非アクティブにしないと決定した場合、フィルタのアクティベーション タイムアウトが新たにゼロから再びカウントされます。動的フィルタの非アクティベーションの基準を変更するには、**filter-termination** コマンドを使用します。詳細については、P.7-38 の「動的フィルタの非アクティブ化」を参照してください。

ポリシーのタイムアウトを設定するには、次のコマンドを入力します。

timeout {**forever** | *timeout*}

表 8-12 で、**timeout** コマンドの引数とキーワードについて説明します。

表 8-12　timeout コマンドの引数とキーワード

パラメータ	説明
forever	無限の期間。
timeout	ポリシーによって生成される動的フィルタがアクティブである最小期間を指定する 1 ～ 3,000,000 の整数。

ポリシーのグループのタイムアウトを同時に変更できます。この場合、ゾーン設定モードで **policy set-timeout** コマンドを使用します。

ポリシーのアクションの設定

アクション パラメータは、しきい値超過が発生したときにポリシーが実行するアクションのタイプを定義します。ポリシーのアクションを設定するには、次のコマンドを入力します。

action *policy-action*

表 8-13 で、ポリシーのアクションについて説明します。

表 8-13　ポリシーのアクション

ポリシーのアクション	簡単な説明
block-unauthenticated	事前ハンドシェイクなしの ACK など、スプーフィング防止メカニズムによって認証されなかったトラフィックをブロックするフィルタを追加します。
filter/strong	トラフィックを強化保護モジュール メカニズムに誘導するフィルタを追加します。
to-user-filters	トラフィックをユーザ フィルタに誘導するフィルタを追加します。
filter/drop	特定のトラフィックをドロップするように Guard モジュールを誘導するフィルタを追加します。
redirect/zombie	redirect というアクションを持つすべてのユーザ フィルタの認証機能を強化するフィルタを追加します。
notify	しきい値を超過するとユーザに通知します。

ポリシーのグループのアクションを同時に変更するには、ゾーン設定モードで **policy set-action** コマンドを使用します。

（注） すべてのアクションがすべてのポリシーで有効なわけではありません。特定のポリシーに有効ではないアクションに対するポリシーのアクションを変更すると、Guard モジュールはエラー メッセージを表示します。

次の例は、*dns_tcp* に関連するすべてのポリシーのアクションを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# policy dns_tcp/ set-action filter/drop
set action of dns_tcp/ to filter/drop:
16 policy actions set.
```

ポリシーのインタラクティブ ステータスの設定

インタラクティブ ステータスのパラメータは、ポリシーによって作成される保留動的フィルタのインタラクティブ ステータスを定義します。インタラクティブ ステータスは、保護をイネーブルにし、ゾーンがインタラクティブ保護モードである場合にのみゾーンに適用できます。詳細については、第 9 章「インタラクティブ保護モード」を参照してください。

現在保護されているゾーンの推奨事項のインタラクティブ ステータスを **always-accept** または **always-ignore** に設定している場合、ポリシーの保留動的フィルタのステータスを変更するには、**interactive-status** コマンドを使用します。

たとえば、推奨事項のステータスを *always-accept* に設定すると、推奨事項と推奨事項の保留動的フィルタが表示されなくなります。推奨事項または推奨事項によって生成される保留動的フィルタを無視することを選択するには、ポリシーのインタラクティブ ステータスを **interactive** または **always-accept** に変更します。

ポリシーのインタラクティブ ステータスを設定するには、次のコマンドを入力します。

interactive-status {**always-ignore** | **always-accept** | **interactive**}

表 8-14 で、**interactive-status** コマンドのキーワードについて説明します。

表 8-14　interactive-status コマンドのキーワード

パラメータ	説明
always-accept	ポリシーによって生成される動的フィルタを自動的に受け入れます。これは、ポリシーによって新しい推奨事項が生成されると必ず、自動的に適用されます。 Guard モジュールはこのような推奨事項を表示しません。
always-ignore	ポリシーによって生成される動的フィルタを自動的に無視します。ポリシーは、いったんしきい値を超過すると推奨事項を生成しません。 Guard モジュールはこのような推奨事項を表示しません。
interactive	ポリシーによって生成される動的フィルタを受け入れるか無視するか、ユーザの決定を待ちます。 Guard モジュールはこのような動的フィルタを推奨事項の一部として表示します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/pkts/src_ip#
interactive-status always-accept
```

ポリシーの監視

ポリシーを監視して、ポリシーがゾーンのトラフィック量やサービスにどの程度適しているかを確認できます。

この項では、次のトピックについて取り上げます。

- ポリシーの表示
- ポリシーの統計情報の表示

ポリシーの表示

ゾーンのポリシーを表示して、ポリシーがゾーンのトラフィック特性に適しているかどうかを確認できます。ゾーンに構築されたポリシーを表示して、これらのポリシーがゾーンのトラフィックの特性に合せて適切に調整されていることを確認する必要があります。このリストに表示されるポリシーだけを設定できます。

Guard モジュールは、現在のゾーン ポリシーだけを表示します。ポリシー構築フェーズ中にポリシー テンプレートがディセーブルであった場合、Guard モジュールはそのポリシー テンプレートからポリシーを作成しないため、**show policies** コマンドを発行してもそのポリシーは表示されません。

ゾーンのポリシーを表示するには、次のコマンドを入力します。

show policies *policy-path*

policy-path 引数には、ポリシーのグループを指定します。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。すべてのポリシーの統計情報を表示するには、アスタリスク（*）を入力します。

表 8-15 で、**show policies** コマンド出力のフィールドについて説明します。

表 8-15　show policies コマンド出力のフィールド説明

フィールド	簡単な説明
Policy	ポリシー名を示します。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。
State	ポリシーの状態を示します。詳細については、P.8-22 の「ポリシーの状態の変更」を参照してください。 act は active、inact は inactive、disab は disabled を指します。
IStatus	ポリシーのインタラクティブ ステータスを示します。詳細については、P.8-32 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。 a-accept は always-accept、a-ignor は always-ignore、interac は interactive を指します。
Threshold	ポリシーのしきい値を示します。このしきい値を超過すると、Guard モジュールはアクションを実行してゾーンを保護します。詳細については、P.8-23 の「ポリシーのしきい値の設定」を参照してください。
Proxy	ポリシーのプロキシしきい値を示します。詳細については、P.8-29 の「プロキシしきい値の設定」を参照してください。
List	ポリシーに定義されている特定の IP しきい値の数を示します。詳細については、P.8-28 の「特定の IP しきい値の設定」を参照してください。
Action	しきい値超過が発生した場合にポリシーが実行するアクションを示します。詳細については、P.8-31 の「ポリシーのアクションの設定」を参照してください。
Timeout	ポリシーのアクションが有効な最小期間を示します。Guard モジュールは、フィルタの終了しきい値に従って、そのポリシーによって作成された動的フィルタを非アクティブにするかどうかを決定します。詳細については、P.8-30 の「ポリシーのタイムアウトの設定」を参照してください。

ポリシーの統計情報の表示

1 つのポリシーまたはポリシーのグループを通過するトラフィックのレートを表示できます。サービス タイプおよびトラフィック量がゾーンのトラフィックを表すかどうかを判断できます。Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。レートは、トラフィックのサンプルに基づいて計算されます。

ポリシーの統計情報を表示するには、次のコマンドを入力します。

show policies *policy-path* **statistics** [*num-entries*]

表 8-16 で、**show policies statistics** コマンド出力の引数について説明します。

表 8-16　show policies statistics コマンドの引数

パラメータ	説明
policy-path	統計情報を表示するポリシーのグループを指定します。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。すべてのポリシーの統計情報を表示するには、アスタリスク（*）を入力します。
num-entries	表示するエントリの数を指定します。1 ～ 100 の数字を入力します。Guard モジュールは、最大の値を持つポリシーを表示します。

Guard モジュールは、4 つのテーブルに情報を表示します。各テーブルの情報は値によってソートされ、最大の値が一番上に表示されます。

表 8-17 で、**show policies statistics** コマンド出力テーブルのフィールドについて説明します。

表 8-17　show policies statistics コマンド出力テーブルのフィールド説明

テーブル	説明
すべての出力テーブルのフィールド	
Key	キー（ポリシーの集約に使用されたトラフィック特性）を示します。 たとえば、ポリシー *tcp_services/any/analysis/syns/dst_ip* の場合、キーは宛先 IP アドレス（dst_ip）です。ポリシーの集約に使用されたトラフィック特性が global である場合、キーには N/A と表示されます。 詳細については、表 8-7 を参照してください。
Policy	ポリシー名を示します。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。
1 つの出力テーブルのフィールド	
Rate	ポリシーを通過するトラフィックのレートを pps で示します。レートは、トラフィックのサンプルに基づいて計算されます。
Connection	同時接続の数を示します。この情報は、tcp_connections ポリシーおよび次のパケット タイプについてのみ表示されます。 • **in_nodata_conns**：分析保護モジュールの場合 • **in_conns**：強化保護モジュールの場合
Ratio	SYN フラグの付いたパケット数と FIN/RST フラグの付いたパケット数の比率を示します。この情報は、syn_by_fin ポリシーだけで使用できます。

（注） Guard モジュールは、データを含まないテーブルを表示しません。

スナップショットを使用したラーニング プロセスの結果の確認

ラーニング プロセス中の任意の段階でラーニング パラメータ（サービス、しきい値、その他のポリシー関連データ）のスナップショットを保存して、後で確認できます。2 つのゾーンのラーニング パラメータまたはスナップショットを比較して、ラーニング プロセスの結果を確認し、ポリシー、サービス、およびしきい値の違いをトレースできます。

ラーニング プロセス中、数時間ごとにスナップショットを保存することをお勧めします。ラーニング プロセス中に攻撃が発生した場合は、スナップショット ポリシーをゾーンに使用できます。スナップショットは手動で取得するか、または Guard モジュールを自動的に指定した間隔でスナップショットを取得するように設定できます。Guard モジュールは、各ゾーンにスナップショットを 100 個まで保存します。以前のスナップショットは新しいスナップショットに置き換えられます。

スナップショットからポリシーをコピーすることで、必要に応じて、以前のラーニングの結果に基づいてゾーンを設定できます。

この項では、次のトピックについて取り上げます。

- スナップショットの作成
- ラーニングの結果の比較
- スナップショットの表示
- ポリシーのコピー

スナップショットの作成

ゾーンのラーニング パラメータのスナップショットを 1 つ保存することができます。または、自動的に指定した間隔でスナップショットを取得するように Guard モジュールを設定できます。Guard モジュールは、スナップショットが撮られている間も、ラーニング フェーズを続行します。

自動的に指定した間隔でスナップショットを取得するように Guard モジュールを設定する方法の詳細については、P.6-25 の「定期的なアクションの設定」を参照してください。

ゾーンのラーニング パラメータのスナップショットを 1 つ保存するには、ゾーン設定モードで次のコマンドを入力します。

```
snapshot [threshold-selection {new-thresholds | max-thresholds |
cur-thresholds | weighted calc-weight}]
```

表 8-18 で、**snapshot** コマンドの引数とキーワードについて説明します。

表 8-18　snapshot コマンドの引数とキーワード

パラメータ	説明
threshold-selection	Guard モジュールがスナップショットのしきい値の計算に使用する方式を設定します。デフォルトでは、Guard モジュールは **learning-params threshold-selection** コマンドで定義されたゾーンのしきい値選択方式を使用します。ゾーンのデフォルトのしきい値選択方式は、**max-thresholds** です。
new-thresholds	Guard モジュールは、ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	Guard モジュールは、ポリシーの現在のしきい値とラーニング済みのしきい値とを比較し、2 つのうちで大きな方の値をゾーン設定に保存します。 これがデフォルトの方式です。
weighted *calc-weight*	Guard モジュールは、保存するポリシーしきい値を次の式に基づいて計算します。 しきい値 = (新しいしきい値 * 計算された重み + 現在のしきい値 * (100 - 計算された重み)) / 100
cur-thresholds	Guard モジュールは、ラーニング プロセスの新しいしきい値を無視し、現在のポリシーのしきい値をスナップショットに保存します。この方式は、バックアップの目的で使用できます。

snapshot コマンドを使用すると、ゾーンのラーニング プロセスの結果が保存されます。この結果には、ゾーンのポリシー、サービス、およびしきい値が含まれます。スナップショットのパラメータを確認するか、2 つのスナップショットを比較するか、またはスナップショットのパラメータを新しいゾーンにコピーし終わったら、スナップショットを削除できます。

現在のゾーン ポリシーは、**snapshot threshold-selection cur-thresholds** コマンドを使用していつでもバックアップできます。

次の例は、ポリシーの現在のしきい値とラーニング プロセスの新しいしきい値のうちで最も大きい値をしきい値として持つスナップショットを作成する方法を示しています。

```
user@GUARD-conf-zone-scannet# snapshot threshold-selection
max-thresholds
```

グローバル モードでスナップショットを 1 つ保存するには、**snapshot** *zone-name* [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *weight*}] コマンドを使用します。

スナップショットを削除するには、**no snapshot** コマンドを使用します。

ラーニングの結果の比較

2 つのスナップショットまたはゾーンのラーニングの結果を比較して、ポリシー、サービス、およびしきい値の違いをトレースできます。

この項では、次のトピックについて取り上げます。

- スナップショットの比較
- ゾーンの比較

スナップショットの比較

2 つのスナップショットを比較するには、ゾーン設定モードで次のコマンドを入力します。

diff snapshots *snapshot-id snapshot-id* [***percent***]

表 8-19 で、**diff** コマンドの引数について説明します。

表 8-19　diff コマンドの引数

パラメータ	説明
snapshot-id	比較対象のラーニング パラメータを持つスナップショットの ID。ゾーンのスナップショットのリストを表示するには、**show snapshots** コマンドを使用します。
percent	（オプション）トレースしきい値。Guard は、2 つのスナップショットを比較した場合、相違点がここに指定したしきい値を超えているポリシーしきい値パラメータをすべてトレースします。デフォルトのパーセンテージは 100% で、Guard は 2 つのスナップショットにおける相違をすべてトレースします。

次の例は、ゾーンのスナップショットを表示し、最新の 2 つのスナップショットを比較する方法を示しています。

```
user@GUARD-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
3    Feb 10 11:01:50
user@GUARD-conf-zone-scannet# diff 2 3
```

グローバル モードでスナップショットを比較するには、**diff** *zone-name* **snapshots** *snapshot-id snapshot-id* [*percent*] コマンドを使用します。

ゾーンの比較

2 つのゾーンのラーニング パラメータを比較するには、グローバル モードまたは設定モードで次のコマンドを入力します。

diff *zone-name zone-name* [***percent***]

表 8-20 で、**diff** コマンドの引数について説明します。

表 8-20　diff コマンドの引数

パラメータ	説明
zone-name	比較対象のラーニング パラメータを持つゾーンの名前。
percent	（オプション）トレースしきい値。Guard は、2 つのゾーンを比較した場合、相違点がここに指定したしきい値を超えているポリシーしきい値パラメータをすべてトレースします。デフォルトのパーセンテージは 100% で、Guard は 2 つのゾーンにおける相違をすべてトレースします。

次の例を参考にしてください。

```
user@GUARD# diff scannet scannet-mailserver
```

スナップショットの表示

ゾーンのラーニングの結果を明確に把握するために、ゾーンのスナップショットまたはスナップショット パラメータのリストを表示できます。

ゾーンのスナップショットを表示するには、次のコマンドを入力します。

show snapshots [*snapshot-id* [**policies** *policy-path*]]

表 8-21 で、**show snapshots** コマンドの引数とキーワードについて説明します。

表 8-21　show snapshots コマンドの引数とキーワード

パラメータ	説明
snapshots	ゾーンのスナップショットを表示します。スナップショットの ID を指定しない場合、デフォルトでは、ゾーンのスナップショットすべてのリストが表示されます。
snapshot-id	表示対象のラーニング パラメータを持つスナップショットの ID。ポリシーを指定しない場合、デフォルトでは、ゾーンのスナップショットすべてのリストが表示されます。スナップショットの ID を表示するには、**show snapshots** コマンドを使用します。
policy-path	表示対象のポリシーのグループを指定します。詳細については、P.8-2 の「ポリシー パス構造」を参照してください。

グローバル モードでスナップショットを比較するには、**show zone** *zone-name* **snapshots** [*snapshot-id* [**policies** *policy-path*]] コマンドを使用します。

次の例は、ゾーンのスナップショットのリストを表示し、次にスナップショット *2* の *dns_tcp* に関連するポリシーを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@GUARD-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

show zone *zone-name* **snapshots** *snapshot-id* **policies** *policy-path* コマンドの出力のフィールドは、**show policies** コマンドの出力のフィールドと同じです。詳細については、P.8-34 の「ポリシーの表示」を参照してください。

表 8-22 で、**show snapshots** コマンド出力のフィールドについて説明します。

表 8-22　show snapshots コマンド出力のフィールドの説明

フィールド	説明
ID	スナップショットの ID。
Time	スナップショットが取得された日時。

ポリシーのコピー

ポリシーの設定または部分的な設定を現在のゾーンにコピーできます。

次の情報をコピーできます。

- サービスをコピーする：ソース　ゾーンから別のゾーンにサービスをコピーできます。このようにして、サービスを検出するためにポリシー構築フェーズを適用せずに、ゾーンのポリシーを設定できます。サービスをゾーンにコピーするには、まず、そのゾーンが同様のトラフィック パターンを持つことを確認します。
- ポリシー パラメータをコピーする：ポリシー パラメータを、ゾーンのスナップショットの 1 つが持つポリシー パラメータに置き換えることができます。このようにして、以前のラーニングの結果に戻すことができます。Guard モジュールは、既存ポリシーのパラメータだけをコピーします。

ゾーンのポリシーをコピーするには、ゾーン設定モードで次のコマンドを入力します。

copy-policies {***snapshot-id*** | *src-zone-name* [*service-path*]}

表 8-23 で、**copy-policies** コマンドの引数とキーワードについて説明します。

表 8-23　copy-policies コマンドの引数とキーワード

パラメータ	説明
snapshot-id	ポリシーのコピー元のスナップショットの ID。スナップショットの ID を表示するには、**show snapshots** コマンドを使用します。
src-zone-name	サービス ポリシーのコピー元のゾーン名。
service-path	コピーされる対象のサービス。サービス パスの形式は、次のいずれかです。 • **policy-template**：ポリシー　テンプレートに関連するすべてのポリシーをコピーします。 • **policy-template/service-num**：ポリシー テンプレートおよび指定のサービスに関連するすべてのポリシーをコピーします。 デフォルトでは、すべてのポリシーとサービスがコピーされます。

次の例は、ポリシー テンプレート *tcp_connections* に関連するすべてのサービスを、ゾーン *webnet* から現在のゾーン *scannet* にコピーする方法を示しています。

```
user@GUARD-conf-zone-scannet# copy-policies webnet tcp_connections/
```

次の例は、ゾーンのスナップショットのリストを表示し、次に ID が *2* のスナップショットからポリシーをコピーする方法を示しています。

```
user@GUARD-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@GUARD-conf-zone-scannet# copy-policies 2
```

CHAPTER 9

インタラクティブ保護モード

ゾーン保護をイネーブルにすると、Cisco Anomaly Guard Module（Guard モジュール）はゾーンのトラフィックを分析して、超過しているポリシーのしきい値を検索します。ポリシーのしきい値を超過したことを検出すると、トラフィックを分析し、トラフィックを処理するためのフィルタのセット（動的フィルタ）を作成します。動的フィルタは、自動またはインタラクティブのどちらでもアクティブにできます。この章では、インタラクティブ保護モードについて説明します。この章は、次の項で構成されています。

- 概要
- インタラクティブ保護モードのアクティブ化
- インタラクティブ保護モードの非アクティブ化
- 推奨事項の表示
- 推奨事項の管理

概要

DDoS 攻撃が開始されると、Guard モジュールのポリシーは動的フィルタを作成します。ゾーンがインタラクティブ保護モードである場合、Guard モジュールはこのような動的フィルタを自動的にアクティブにせず、ユーザの決定を待ちます。このようなフィルタは、保留動的フィルタと呼ばれます。推奨事項は、フィルタを生成したポリシーに応じた保留フィルタのサマリーです。この情報には、推奨事項を提示したポリシーの名前、ポリシーのアクティベーションの原因となったトラフィック異常に関するデータ、保留動的フィルタの数、および推奨アクションが含まれています。どの保留動的フィルタを受け入れるか、無視するか、または自動アクティベーションに向けるかを決定することにより、攻撃が進行しているときに講じる対策をより強く制御できます。

Guard は、インタラクティブ保護モードである限り、保留動的フィルタの生成を続けて、ゾーンを保護します。ゾーンの保護中いつでもインタラクティブ保護モードをアクティブにできますが、Guard がインタラクティブ保護モードで、ゾーンに対する DDoS 攻撃が進行中である場合にだけ、推奨事項およびその保留動的フィルタを表示できます。インタラクティブ保護モードは、ゾーンの定義時、またはゾーン保護の開始前後に設定できます。

1000 個を超える保留動的フィルタがある場合、Guard モジュールは次のように動作します。

- ゾーンを非アクティブにして自動保護モードで再度アクティブにするよう指示するエラー メッセージを表示する。
- ゾーンのログ　ファイルおよびレポートに推奨事項を記録してから、推奨事項を廃棄する。

新しい推奨事項が利用可能になっている場合、Guard モジュールは通知を表示しません。推奨事項を追跡するには、次のいずれかを行います。

- ゾーン設定モードで **show** コマンドを使用して、ゾーンのステータスを表示する。
- **event monitor** コマンドを使用して、新しい保留動的フィルタの作成時に通知を受け取る。
- 外部 syslog サーバを使用して、新しい保留動的フィルタの通知を受け取る。

いつでもインタラクティブ保護モードを停止して、自動保護モードに戻ることができます。Guard モジュールは、インタラクティブ保護モード中の決定をすべて無視し、現在の保留動的フィルタをすべて受け入れます。ポリシーは、動的フィルタを自動的に生成してアクティブにするという役割を再開します（第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください）。

インタラクティブ保護モードのアクティブ化

既存のゾーンのインタラクティブ保護モードをアクティブにするには、ゾーン設定モードで **interactive** と入力します。

インタラクティブ保護モードに設定された新しいゾーンを作成するには、設定モードで次のコマンドを入力します。

zone *new-zone-name* **interactive**

new-zone-name 引数には、新しいゾーンの名前を指定します。ゾーン名は英数字の文字列とし、必ず英字で入力を開始してください。スペースは使用できません。また、63 文字以内で入力してください。

次の例を参考にしてください。

```
user@GUARD-conf# zone scannew interactive
```

インタラクティブ保護モードに設定された新しいゾーンが、デフォルト ゾーン テンプレートで作成されます。詳細については、第 6 章「ゾーンの設定」を参照してください。

インタラクティブ保護モードの非アクティブ化

インタラクティブ保護モードを非アクティブにするには、**no interactive** コマンドを使用します。インタラクティブ保護モードを非アクティブにすると、ポリシーのインタラクティブ ステータスが **always-accept** になります。

推奨事項の表示

ゾーンのすべての推奨事項のリスト、保留動的フィルタのリスト、または特定の推奨事項を表示するには、**show recommendations** コマンドを使用します。次のコマンドを入力します。

show recommendations [*recommendation-id*] [**pending-filters**]

表 9-1 で、**show recommendations** コマンドのキーワードと引数について説明します。

表 9-1　show recommendations コマンドのキーワードと引数

パラメータ	説明
recommendation-id	（オプション）特定の推奨事項の ID。
pending-filters	（オプション）特定の推奨事項の保留フィルタのリストを表示します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show recommendations
```

表 9-2 で、**show recommendations** コマンド出力のフィールドについて説明します。

表 9-2　show recommendations コマンドのフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。
Min current rate	最小攻撃レート（pps）。 複数の保留動的フィルタを持つ推奨事項の場合、最小攻撃レートの保留動的フィルタのレートが表示されます。
Max current rate	最大攻撃レート（pps）。 複数の保留動的フィルタを持つ推奨事項の場合、最大攻撃レートの保留動的フィルタのレートが表示されます。
No. of pending-filters	ポリシーしきい値の超過が発生したために作成された保留動的フィルタの数。
Recommended action	推奨されているアクション。推奨事項を受け入れると、このアクションが実行されます。

特定の推奨事項の保留フィルタを表示する前に、すべての推奨事項とその ID のリストを表示するには、**show recommendations** コマンドを使用します。

表 9-3 で、**show recommendations pending-filters** コマンド出力のフィールドについて説明します。

表 9-3　show recommendations pending-filters コマンドのフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値（pps）。
Pending-filter-id	保留動的フィルタの識別番号。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。
Triggering Rate	保留動的フィルタの作成をトリガーした攻撃レート（pps）。
Current rate	現在の攻撃レート（pps）。
Recommended action	推奨されているアクション。推奨事項を受け入れると、このアクションが実行されます。
Action flow	保留動的フィルタを受け入れた場合にそのフィルタで処理される、ゾーンへのトラフィック フローの特性。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

パラメータの値が * となっている場合は、次のいずれかの状態であることを示します。

- 値が特定されていない。
- パラメータに対して複数の値が測定された。

（注） Guard がインタラクティブ保護モードで、ゾーンに対する DDoS 攻撃が進行中である場合にだけ、推奨事項およびその保留動的フィルタを表示できます。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show recommendations 135 pending-filters
```

推奨事項の管理

推奨事項をアクティブにするかどうかを決定できます。すべての推奨事項、特定の推奨事項、または特定の保留動的フィルタに対して決定を行うことができます。その決定によって、ポリシーの保留動的フィルタが動的フィルタになるかどうか、およびその期間が決まります。

特定のポリシーの保留動的フィルタを自動的にアクティブにするよう Guard モジュールに指示できます。また、ポリシーによって推奨事項が生成されないよう Guard モジュールに指示することもできます。DDoS 攻撃が続行し、その特性を変更している間、Guard モジュールのポリシーは推奨事項を生成し続けます。

決定を確認するには、決定を行った後にゾーンのステータスを表示します。

（注） 推奨事項を受け入れると、受け入れた推奨事項と同じまたは受け入れた推奨事項に含まれるフローを持ち、アクションとタイムアウトが同じである、その他の推奨事項も同様に受け入れられます。Guard モジュールはこのような推奨事項を削除します。

ゾーンの推奨事項に関して決定を行うには、ゾーン設定モードで **recommendation** コマンドを使用します。次のコマンドを入力します。

recommendation *recommendation-id* [**pending-filters** *pending-filter-id*] *decision* [*timeout*]

表 9-4 で、**recommendation** コマンドの引数とキーワードについて説明します。

表 9-4　recommendation コマンドの引数とキーワード

パラメータ	説明
recommendation-id	特定の推奨事項の識別番号。アスタリスク（*）は、すべての推奨事項を示すワイルドカードです。
pending-filter-id	（オプション）特定の保留動的フィルタの ID。
decision	推奨事項に対して実行するアクション。指定できる値は、次のとおりです。 • **accept**：特定の推奨事項を受け入れます。保留動的フィルタは、動的フィルタになります。 • **always-accept**：特定の推奨事項を受け入れます。この決定は、推奨ポリシーによって新しい推奨事項が生成されると必ず、自動的に適用されます。保留動的フィルタは、自動的に動的フィルタになります。 このアクションを実行すると、Guard はこのような推奨事項を表示しなくなります。 • **always-ignore**：特定の推奨事項を無視します。動的フィルタも保留フィルタも生成されません。この決定は、ポリシーによって生成される将来のすべての推奨事項に自動的に適用されます。 推奨事項を常に無視するように決定した場合は、Guard が推奨事項を表示しなくなります。
timeout	（オプション）決定が適用される期間。指定できる値は、次のとおりです。 • **forever**：保護が有効である限り、Guard が、推奨事項によって生成された動的フィルタ（P.7-31 の「動的フィルタの設定」を参照）をアクティブにします。 • *new-timeout*：定義した期間中、Guard が、ポリシーによって生成された動的フィルタ（詳細については、P.7-31 の「動的フィルタの設定」を参照）をアクティブにします。この期間は秒で測定されます。

特定のポリシーまたはポリシーの任意の部分のインタラクティブ ステータスを設定し、ポリシーのその部分が推奨事項と保留動的フィルタを生成するかどうかを決定できます。詳細については、P.8-32 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。この設定により、さらに強力な制御が可能になり、ポリシーをトラフィック フローに、よりよく適合させることができます。

Guard は、**always-accept** および **always-ignore** の推奨事項を表示しません。推奨事項を常に無視するまたは常に受け入れると決定した場合、その決定は、推奨事項を作成したポリシーのインタラクティブ ステータスの一部となります。

ポリシーをディセーブルまたは非アクティブにして、ポリシーが推奨事項と保留動的フィルタを生成しないようにすることができます。ポリシーをディセーブルまたは非アクティブにするには、**state** コマンドを使用します。詳細については、P.8-22 の「ポリシーの状態の変更」を参照してください。

次の例は、*analysis*（分析）保護モジュールを使用する、サービス *53* の *dns_tcp* ポリシー テンプレートのインタラクティブ ステータスを設定しています。

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/#
interactive-status always-accept
```

詳細については、P.8-14 の「ポリシー パスのセクションについて」を参照してください。

CHAPTER 10

攻撃レポート

この章では、Cisco Anomaly Guard Module（Guard モジュール）が生成する攻撃レポートについて説明します。この章には、次の項があります。

- レポートのレイアウトについて
- レポートのパラメータについて
- 攻撃レポートの表示
- 攻撃レポートのエクスポート

レポートのレイアウトについて

Guard は、攻撃を明確に把握するために役立つ、各ゾーンの攻撃レポートを提供します。攻撃の開始は Guard によって最初に動的フィルタが生成されたときで、攻撃の終了は動的フィルタが使用されなくなり新しい動的フィルタが追加されなくなったときです。レポートには、攻撃の詳細がセクションに分かれて記載されます。各セクションには、攻撃中のトラフィック フローの異なる面が記載されます。過去の攻撃および進行中の攻撃のレポートを表示できます。また、レポートを FTP サーバまたは セキュア FTP（SFTP）サーバにエクスポートすることもできます。

レポートには、次のセクションがあります。

- General Details
- Attack Statistics
- Dropped/ Replied Packets
- Detected Anomalies
- Mitigated Attacks
- Zombies：このセクションは、**show reports details** コマンドおよび **show zombies** コマンドを発行した場合にだけ表示されます。

General Details

攻撃レポートの General Details セクションには、攻撃に関する一般的な情報が記載されます。表 10-1 で、レポートのこのセクションのフィールドについて説明します。

表 10-1　攻撃レポートの General Details セクションのフィールド説明

フィールド	説明
Report ID	レポートの識別番号。
Attack Start	攻撃が開始された日時を表示します。
Attack End	攻撃が終了した日時を表示します。*Attack in progress* は、進行中の攻撃があることを示します。
Attack Duration	攻撃の期間を表示します。

Attack Statistics

Attack Statistics セクションには、さまざまなパケットのゾーン トラフィック フローの一般的な分析が記載されます。表 10-2 で、パケット タイプについて説明します。

表 10-2　パケット タイプ

タイプ	説明
Received	宛先変更されたトラフィックの合計量を示します。
Forwarded	Guard モジュールがゾーンに転送した正当なトラフィックを示します。
Replied	検証の試行で Guard モジュールのスプーフィング防止メカニズムおよびゾンビ防止メカニズムが送信元に返送したトラフィックを示します。
Dropped	Guard モジュールがドロップしたトラフィックを示します。

Dropped/ Replied Packets

攻撃レポートの Dropped/Replied Packets セクションでは、検証の試行で Guard モジュールによってドロップされたパケットおよび送信元に返送されたパケットが分析されます。レポートでは、パケットがタイプ（スプーフィングまたは不正な形式）および処理メカニズム（フィルタ タイプまたはレート リミット保護モジュール）によって分類されます。表 10-3 で、ドロップされたパケットおよび返送されたパケットのさまざまなタイプについて説明します。

表 10-3　ドロップされたパケットおよび返送されたパケットのタイプ

タイプ	説明
Rate Limiter	ゾーンのレート リミット保護モジュールによってドロップされたパケットを示します。これらのパケットは、ユーザ フィルタのレート リミット パラメータ、およびゾーンの **rate-limit** コマンドによって定義されます。
Flex-Content Filters	フレックスコンテンツ フィルタによってドロップされたパケットを示します。
User Filters	ユーザ フィルタによってドロップされたパケットを示します。
Dynamic Filters	動的フィルタによってドロップされたパケットを示します。
Spoofed	Guard モジュールによって、スプーフィングされたパケットまたはゾンビが発信したパケットであると識別されたため、ゾーンに転送されなかったパケットを示します。スプーフィング パケットは、応答された（返送された）パケットのうち、応答を受信しなかったパケットです。
Malformed	不正な形式の構造であるため、または Guard モジュールのスプーフィング防止メカニズムが原因で、不正な形式であると分析されたパケットを示します。

Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Guard モジュールがゾーンのトラフィックで検出したトラフィック異常の詳細が記載されます。動的フィルタの作成を必要とするフローは、トラフィック異常として分類されます。これらの異常は頻繁に発生するものではなく、組織的な DDoS 攻撃に変化する可能性があります。Guard は、同じタイプおよび同じフロー パラメータ（送信元 IP アドレスや宛先ポートなど）の異常を 1 つの異常タイプにまとめます。表 10-4 で、検出された異常のさまざまなタイプについて説明します。

表 10-4　検出された異常のタイプ

タイプ	説明
dns (tcp)	攻撃している DNS-TCP プロトコル フロー。
dns (udp)	攻撃している DNS-UDP プロトコル フロー。
fragments	断片化されたトラフィックが異常な量であることが検出されたフロー。
http	異常な HTTP トラフィック フロー。
ip_scan	多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。
other_protocols	攻撃している TCP/UDP 以外のプロトコル フロー。
port_scan	多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。
tcp_connections	データを保持している（または保持していない）、異常な数の TCP 同時接続が検出されたフロー。
tcp_incoming	ゾーンがサーバである場合に、TCP サービスを攻撃していることが検出されたフロー。
tcp_outgoing	ゾーンがクライアントである場合に、ゾーンによって開始された接続に対する SYN-ACK フラッドまたは他のパケット攻撃で構成されていることが検出されたフロー。
tcp_ratio	異なるタイプの TCP パケット間（たとえば、SYN パケット対 FIN/RST パケット）の比率が異常であることが検出されたフロー。
udp	攻撃している UDP プロトコル フロー。

表 10-4　検出された異常のタイプ（続き）

タイプ	説明
unauthenticated_tcp	Guard のスプーフィング防止メカニズムが認証に成功しなかったことが検出されたフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。
user	ユーザ定義によって検出された異常なフロー。

Mitigated Attacks

攻撃レポートの Mitigated Attacks セクションには、Guard モジュールがゾーンを保護する（攻撃を軽減する）ために実行した処置が詳細に記載されます。このレポートには、軽減のタイミングおよび軽減された攻撃のタイプの詳細が記載されます。Guard モジュールは、使用したメカニズムに応じて軽減のタイプを定義します。このメカニズムは、攻撃のタイプとサブタイプを示します。

たとえば、Guard モジュールが syn パケットの攻撃フローに対して基本的なスプーフィング防止メカニズムを使用した場合、軽減された攻撃は **spoofed/tcp_syn_basic** と表示されます。spoofed は攻撃のタイプを示し、tcp_syn_basic はサブタイプを示します。

軽減された攻撃には、次の 5 つのタイプがあります。

- スプーフィング利用
- ゾンビ
- クライアント攻撃
- ユーザ定義
- 不正な形式のパケット

スプーフィング利用

スプーフィングを利用した攻撃には、スプーフィングされた送信元からの DDoS 攻撃であると識別されるすべてのトラフィック異常が含まれます。表 10-5 で、スプーフィングを利用した攻撃のさまざまなタイプについて説明します。

表 10-5　スプーフィングを利用した攻撃のタイプ

攻撃のタイプ	説明
spoofed/tcp_syn (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった SYN パケットのフラッド。
spoofed/tcp_syn (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった SYN パケットのフラッド。
spoofed/tcp_syn_ack (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった syn_ack パケットのフラッド。
spoofed/tcp_syn_ack (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった syn_ack パケットのフラッド。
spoofed/tcp_incoming (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかったトラフィックのフラッド。
spoofed/tcp_incoming (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかったトラフィックのフラッド。
spoofed/tcp_outgoing (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信トラフィックのフラッド。
spoofed/udp (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった UDP トラフィックのフラッド。
spoofed/udp (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった UDP トラフィックのフラッド。
spoofed/other_protocols	Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、TCP および UDP トラフィック以外のフラッド。
spoofed/tcp_fragments	Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、断片化された TCP パケットのフラッド。

表 10-5　スプーフィングを利用した攻撃のタイプ（続き）

攻撃のタイプ	説明
spoofed/udp_fragments	Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、断片化された UDP パケットのフラッド。
spoofed /other_protocols_fragments	Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、TCP および UDP 以外の断片化されたパケットのフラッド。
spoofed/dns_queries (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった DNS クエリー パケットのフラッド。
spoofed/dns_replies (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信 DNS パケットのフラッド。
spoofed/dns_replies (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信 DNS パケットのフラッド。

ゾンビ

ゾンビ攻撃には、ゾンビによって開始された DDos 攻撃であると識別されるトラフィック異常が含まれます。表 10-6 で、ゾンビ攻撃のタイプについて説明します。

表 10-6　ゾンビ攻撃のタイプ

攻撃のタイプ	説明
zombie/http	Guard モジュールのゾンビ防止メカニズムが認証に成功しなかった、スプーフィングされていないと識別された多くの送信元からの HTTP トラフィックのフラッド。

クライアント攻撃

クライアント攻撃には、スプーフィングされていないすべてのトラフィック異常が含まれます。表 10-7 で、さまざまなタイプのクライアント攻撃について説明します。

表 10-7　クライアント攻撃のタイプ

攻撃のタイプ	説明
client_attack/tcp_connections	データを保持している（または保持していない）、TCP 同時接続数が異常であるフロー。
client_attack/http	HTTP トラフィック フローのフラッド。
client_attack/tcp_ incoming	ゾーンがサーバである場合に、TCP サービスを攻撃しているフラッド。
client_attack/tcp_outgoing	ゾーンが開始した認証済み IP 接続からの攻撃フラッド。
client_attack /unauthenticated_tcp	TCP ハンドシェイクを経ていない ACK、FIN、または他のパケットのフラッド、あるいは Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった TCP 接続。
client_attack/dns (udp)	攻撃している DNS-UDP プロトコル フローのフラッド。
client_attack/dns (tcp)	攻撃している DNS-TCP プロトコル フローのフラッド。
client_attack/udp	攻撃している UDP プロトコル フローのフラッド。
client_attack/other_protocols	攻撃している TCP/UDP 以外のプロトコル フローのフラッド。
client_attack/fragments	断片化されたトラフィックのフラッド。
client_attack/user	ユーザ定義の攻撃のフラッド。この攻撃は、ユーザによって追加された動的フィルタによって定義されます。

ユーザ定義

ユーザ定義攻撃には、ユーザ フィルタによって処理されたすべての異常が含まれます。ユーザ フィルタは、デフォルトで機能するか、またはユーザによって手動で設定されます（詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください）。表 10-8 で、ユーザ定義攻撃のさまざまなタイプについて説明します。

表 10-8　ユーザ定義攻撃のタイプ

攻撃のタイプ	説明
user_defined/ user_filter_rate_limit	ユーザ フィルタ用に定義されたレート リミットを超過したためにドロップされたフラッド。
user_defined/ user_drop_filters	ユーザ フィルタによってドロップされたフラッド。
user_defined/rate_limit	次のいずれかの原因によりドロップされたフラッド。 • ユーザ フィルタ用に定義されたレート リミットを超過した。 • ゾーンの **rate-limit** コマンドによって定義されたレート リミットを超過した。 • 認証されていない TCP RST パケットまたは認証されていない DNS ゾーン転送パケット用に定義された内部レート リミットを超過した。
user_defined/ flex_content_filter	フレックスコンテンツ フィルタによってドロップされたフラッド。

不正な形式のパケット

不正な形式のパケットには、悪意のある不正形式パケットで構成されると識別されたすべてのトラフィック異常が含まれます。表 10-9 で、さまざまなタイプの不正形式パケットについて説明します。

表 10-9　不正形式パケットのタイプ

攻撃のタイプ	説明
malformed_packets /packets_to_proxy_ip	Guard モジュールの プロキシ IP アドレスを攻撃しているフラッド。
malformed_packets /dns_anti_spoofing_algo	Guard モジュールの DNS スプーフィング防止メカニズムの動作が原因の不正な形式のパケットのフラッド。
malformed_packets /dns (queries)	不正な形式の DNS パケットのフラッド。
malformed_packets /dns (short_queries)	短い DNS クエリーのフラッド。
malformed_packets /dns (replies)	不正な形式の DNS 応答のフラッド。
malformed_packets /src ip = dst ip	送信元および宛先としてゾーンの IP アドレスを持つパケットのフラッド。
malformed_packets /zero_header_field	ヘッダーのポート、プロトコル、および IP のフィールドが不正にゼロとなっているパケットのフラッド。

Zombies

ゾンビ攻撃には、ゾンビによって開始された DDoS 攻撃であると識別されたトラフィック異常が含まれます。Guard モジュールの攻撃レポートには、現在ゾーンを攻撃しているゾンビを一覧表示するテーブルが表示されます。現在攻撃しているゾンビのリストを表示するには、**show reports details** コマンドおよび **show zombies** コマンドを使用します。

show zombies コマンド出力のフィールドについては、表 10-15 を参照してください。

レポートのパラメータについて

レポートの異なるセクションには、トラフィック フローの異なる面が記載されます。

表 10-10 で、Attack Statistics および Dropped/ Replied Packets のフィールドについて説明します。

表 10-10　Attack Statistics のフィールド説明

フィールド	説明
Total Packets	攻撃パケットの合計数を示します。
Average pps	平均トラフィック レート（pps）を示します。
Average bps	平均トラフィック レート（bps）を示します。
Max. pps	最大トラフィック レート（pps）を示します。
Max. bps	最大トラフィック レート（bps）を示します。
Percentage	受信パケットの合計数に対する、転送されたパケット、返送されたパケット、およびドロップされたパケットのパーセンテージを示します。

表 10-11 で、Detected Anomalies および Mitigated Attacks のフロー統計情報について説明します。

表 10-11　フロー統計情報のフィールド説明

フィールド	説明
ID	検出された異常の識別番号（ID）を示します。
Start time	異常が検出された日時を示します。
Duration	異常の期間（時間、分、秒）を示します。
Type	異常または軽減された攻撃のタイプを示します。
Triggering Rate	ポリシーのしきい値を超過した異常トラフィック レートを示します。
% Threshold	Triggering rate がポリシーのしきい値を上回っているパーセンテージを示します。

表 10-11　フロー統計情報のフィールド説明（続き）

フィールド	説明
Flow	異常フローおよび軽減された攻撃のフローを示します。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

パラメータの値が * となっている場合は、次のいずれかの状態であることを示します。

- 値が特定されていない。
- 異常のパラメータに対して複数の値が測定された。

任意のパラメータの # という値（数値の前にある）は、そのパラメータに対して測定された値の数を示します。

Guard モジュールはフローの説明の右側に *notify* という値を表示する場合があります。レポートの行に *notify* という値が表示された場合、Guard モジュールはその行が示すトラフィック タイプの通知を生成するだけで、アクションを実行しないことを示します。

攻撃レポートの表示

特定のゾーンの攻撃レポートのリスト、または特定の攻撃の詳細なレポートを表示するには、**show** コマンドを使用します。次のコマンドを入力します。

show reports [*sub-zone-name*] [**current** | *report-id*] [**details**]

表 10-12 で、**show reports** コマンドの引数とキーワードについて説明します。

表 10-12　show reports コマンドの引数とキーワード

パラメータ	説明
sub-zone-name	（オプション）ゾーンから作成されたサブゾーンの名前です。詳細については、P.6-42 の「サブゾーンについて」を参照してください。
current	進行中の攻撃。 進行中の攻撃のビット数およびパケット数は表示されません。進行中の攻撃のレポートでは、パケットとビットのフィールドにゼロ（0）という値が表示されます。
report-id	レポートの識別番号。
details	（オプション）フローおよび攻撃しているゾンビの詳細を表示します。

たとえば、ゾーンに対するすべての攻撃のリストを表示するには、次のコマンドを入力します。

```
user@GUARD-conf-zone-scannet# show reports
```

表 10-13 で、**show reports** コマンド出力のフィールドについて説明します。

表 10-13　show reports コマンド出力のフィールドの説明

フィールド	説明
Report ID	レポートの識別番号。
Attack Start	攻撃が開始された日時。
Attack End	攻撃が終了した日時。*Attack in progress* という値は、進行中の攻撃があることを示します。
Attack Duration	攻撃の期間。
Attack Type	軽減された攻撃のタイプ。使用可能な値は、次のいずれかです。 • **client_attack**：スプーフィング以外のすべてのトラフィック異常。 • **malformed_packets**：悪意のある不正形式パケットと見なされたすべてのトラフィック異常。 • **spoofed**：スプーフィングされた送信元からの DDoS 攻撃と見なされたトラフィック異常。 • **user_defined**：ユーザ フィルタによって処理されたすべての異常。これらのフィルタは、デフォルト設定で動作することも、ユーザが動作を設定することもできます。 • **zombie**：ゾンビが発信元であると見なされたトラフィック異常。 • **hybrid**：特性の異なる複数の攻撃で構成された攻撃。 • **traffic_anomaly**：短期間のみ検出され、軽減を必要としなかった異常。
Malicious Traffic	Guard モジュールによって攻撃の一部と見なされ、ドロップされたパケット数と、正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、Guard モジュールによって開始側のクライアントに応答が送信されたパケット数の合計。

ゾーンに対する現在の攻撃のレポートを表示するには、次のコマンドを入力します。

```
user@GUARD-conf-zone-scannet# show reports current
```

レポートには、次のような出力が表示されます。各セクションの詳細については、P.10-2 の「レポートのレイアウトについて」を参照してください。

```
Attack Start      :   Feb 26 2004 09:58:54
Attack End        :   Attack in progress
Attack Duration   :   00:08:34
```

Attack Statistics:

	Total Packets	Average pps	Average bps	Max pps	Max bps	Percentage
Received	95878	186.53	110977.74	1455.44	914428.24	N/A
Forwarded	53827	104.72	64278.54	1430.85	899196.24	56.14
Replied	1870	3.64	2172.89	23.03	14433.88	1.95
Dropped	40181	78.17	44526.32	96.82	55010.13	41.91

Dropped/Replied Packets:

	Total Packets	Average pps	Average bps	Max pps	Max bps	Percentage
Rate Limiter	0	0	0	0	0	0
Flex-Content Filter	0	0	0	0	0	0
User Filters	0	0	0	0	0	0
Dynamic Filters 40128	78.07	44473.53	96.82	55010.13	99.84	
Spoofed	12	0.02	11.95	0.15	75.29	0.03
Malformed	53	0.1	52.79	1.56	798.12	0.13

```
Detected Anomalies:
ID          Start Time           Duration     Type                Triggering    %Threshold
                                                                  Rate
1           Feb 26 09:58:54      00:08:34     HTTP                997.44        897.44
            Flow: 6 *            *            92.168.100.34  80   no fragments

Mitigated Attacks:
ID          Start Time           Duration     Type                Triggering    %Threshold
                                                                  Rate
1          Feb 26 09:59:40       00:07:59   client_attack/          38            280
                                            tcp_connections
           Flow: 6 (#52)         *          92.168.200.254 80       no fragments
```

検出された異常フローと軽減された攻撃フローに関する詳細なレポート、およびゾンビ攻撃のリストを表示するには、**details** オプションを使用します。

表 10-14 に、詳細なレポートに含まれているフローのフィールドの説明を示します。

表 10-14　詳細なレポートのフローのフィールド説明

フィールド	説明
Detected Flow	動的フィルタが生成される原因となったフローを示します。このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

表 10-14　詳細なレポートのフローのフィールド説明（続き）

フィールド	説明
Action Flow	動的フィルタによって処理されたフローを示します。アクション フローは、検出されたフローよりも範囲が広い可能性があります。たとえば、検出されたフローが特定の送信元 IP アドレスの特定の送信元ポートを示し、アクション フローが特定の送信元 IP アドレスのすべての送信元ポートを示すことがあります。 このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

表 10-15 で、ゾンビ攻撃に関する詳細なレポートのフィールドについて説明します。

表 10-15　ゾンビ攻撃に関するテーブルのフィールドの説明

フィールド	説明
IP	ゾンビの IP アドレス。
Start Time	ゾンビ接続が初めて識別された日時。
Duration	ゾンビ攻撃の期間。
#Requests	ゾンビによって送信された HTTP get 要求の数。

（注） ゾンビ攻撃がない場合は、レポートの Zombies という見出しの下に **Report doesn’t exist** と表示されます。

攻撃レポートのエクスポート

監視および診断のために、攻撃レポートを FTP サーバまたは SFTP サーバにエクスポートできます。テキスト形式または Extensible Markup Language（XML）形式で攻撃レポートをエクスポートできます。

この項では、次のトピックについて取り上げます。

- 攻撃レポートの自動エクスポート
- すべてのゾーンの攻撃レポートのエクスポート
- ゾーン レポートのエクスポート

攻撃レポートの自動エクスポート

攻撃が終了したときに攻撃レポートが XML 形式で自動的にエクスポートされるように Guard モジュールを設定できます。Guard モジュールは、ゾーンに対する攻撃が終了すると、いずれかのゾーンのレポートをエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。設定モードで、次のいずれかのコマンドを入力します。

- **export reports ftp** *server remote-path* [*login*] [*password*]
- **export reports sftp** *server remote-path login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 10-16 で、**export reports** コマンドの引数について説明します。

表 10-16　export reports コマンドの引数

パラメータ	説明
ftp	攻撃レポートを FTP サーバにエクスポートします。
sftp	攻撃レポートを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの保存先ディレクトリの完全パス。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

次の例は、IP アドレス *10.0.0.191* の FTP サーバへの攻撃が終了した後、ログイン名 *user1* とパスワード *password1* を使用してレポートを XML 形式で自動的にエクスポートする方法を示しています。

```
user@GUARD-conf# export reports ftp 10.0.0.191 /root/reports user1
password1
```

すべてのゾーンの攻撃レポートのエクスポート

すべてのゾーンの攻撃レポートをテキストまたは XML 形式でエクスポートできます。レポートを FTP サーバまたは SFTP サーバに手動でコピーするには、**copy reports** コマンドを使用します。

グローバル モードで次のコマンドを入力します。

copy reports [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]

表 10-17 で、**copy reports** コマンドの引数とキーワードについて説明します。

表 10-17　copy reports コマンドの引数とキーワード

パラメータ	説明
xml	（オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。デフォルトでは、レポートはテキスト形式でエクスポートされます。 XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。
details	（オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。
ftp	攻撃レポートを FTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	サーバによるファイルの保存先ディレクトリの完全パス。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

次の例は、ログイン名 *user1* とパスワード *password1* を使用して、Guard モジュールによって処理されたすべての攻撃のリストをテキスト形式で IP アドレス *10.0.0.191* の FTP サーバにコピーする方法を示しています。

```
user@GUARD# copy reports ftp 10.0.0.191 AGMreports.txt user1 password1
```

ゾーン レポートのエクスポート

特定のゾーンの攻撃レポートを FTP サーバにコピーするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **sftp** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 10-18 で、**copy zone reports** コマンドの引数とキーワードについて説明します。

表 10-18　copy zone reports コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
current	（オプション）進行中の攻撃のレポートをエクスポートします（該当する場合）。 デフォルトでは、すべてのゾーン レポートをエクスポートします。
report-id	（オプション）既存のレポートの ID。指定した ID 番号を持つレポートが Guard モジュールによってエクスポートされます。ゾーン攻撃レポートの詳細を表示するには、**show zone reports** コマンドを使用します。 デフォルトでは、すべてのゾーン レポートをエクスポートします。

表 10-18　copy zone reports コマンドの引数とキーワード （続き）

パラメータ	説明
xml	（オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。デフォルトでは、レポートをテキスト形式でエクスポートします。 XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。
details	（オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。
ftp	攻撃レポートを FTP サーバにエクスポートします。
sftp	攻撃レポートを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの保存先ディレクトリの完全パス。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

次の例は、ログイン名 *user1* とパスワード *password1* を使用して IP アドレス *10.0.0.191* の FTP サーバにすべての攻撃レポートをコピーする方法を示しています。

```
user@GUARD# copy zone scannet reports ftp 10.0.0.191
ScannetCurrentReport.txt user1 password1
```

CHAPTER 11

Guard モジュールの診断ツールの使用方法

この章では、Cisco Anomaly Guard Module（Guard モジュール）に関する統計情報や診断を表示する方法について説明します。この章には、次の項があります。

- Guard モジュールの設定の表示
- Guard モジュールのゾーンの表示
- ゾーンのカウンタの表示
- ゾーンのステータスの表示
- Guard モジュールのログの表示
- ネットワーク トラフィックの監視および攻撃のシグニチャの抽出
- 一般的な診断データの表示
- メモリ消費量の表示
- CPU 使用率の表示
- ARP キャッシュの操作
- netstat の使用
- traceroute の使用
- ping の使用
- デバッグ情報の取得
- Guard モジュールの自己保護設定の表示

Guard モジュールの設定の表示

Guard モジュールの設定ファイルを表示することができます。このファイルには、インターフェイスの IP アドレス、デフォルト ゲートウェイ アドレス、設定されたゾーンなど、Guard モジュールの設定に関する情報が含まれています。

Guard モジュールの設定ファイルを表示するには、次のコマンドを入力します。

show running-config [**all** | **Guard module**| **interfaces** *interface-name* | self-protection | zones]]

表 11-1 に、**show running-config** コマンドのキーワードを示します。

表 11-1　show running-config コマンドのキーワード

パラメータ	説明
all	Guard モジュールのすべてのモジュール（Guard モジュール、ゾーン、インターフェイス、および自己保護）の設定ファイルを表示します。
Guard module	Guard モジュールの設定ファイルを表示します。
interfaces	Guard モジュールのインターフェイスの設定ファイルを表示します。インターフェイス名を入力します。
self-protection	Guard モジュールの自己保護の設定を表示します。
zones	すべてのゾーンの設定ファイルを表示します。

次の例を参考にしてください。

```
user@GUARD# show running-config guard
```

設定ファイルは、Guard モジュールを現在の設定値で設定するために実行されるコマンドで構成されています。Guard モジュールの設定ファイルをリモート FTP サーバにエクスポートして、バックアップ用にしたり、別の Guard モジュールにその Guard モジュールの設定パラメータを実装できるようにすることができます。詳細については、P.11-3 の「Guard モジュールのゾーンの表示」を参照してください。

Guard モジュールのゾーンの表示

Guard でゾーンの概要を表示して、アクティブなゾーンやゾーンの現在のステータスを確認できます。ゾーンのリストを表示するには、グローバル モードで **show** コマンドを使用します。表 11-2 で、さまざまなゾーン ステータスについて説明します。

表 11-2　ゾーンのステータス

ステータス	説明
Auto Protect mode	ゾーンは自動保護モードです。ユーザの介入なしに動的フィルタがアクティブになります。 ゾーンが自動保護モードにあり、ポリシーのしきい値を調整するために Guard モジュールがゾーンのトラフィック特性のラーニングを行っている場合、Guard モジュールはゾーン名の横に (+learning) を表示します。
Interactive Protect mode	ゾーンはインタラクティブ保護モードです。動的フィルタは手動でアクティブになります。
Threshold Tuning phase	ゾーンはしきい値調整フェーズです。Guard は、ゾーンのトラフィックを分析して、ポリシー構築フェーズ中に構築されたポリシーのしきい値を定義します。
Policy Construction phase	ゾーンはポリシー構築フェーズです。ゾーンのポリシーが作成されます。
Standby	ゾーンはアクティブではありません。

例

```
user@GUARD# show
```

ゾーンのカウンタの表示

ゾーン カウンタの表示およびゾーン トラフィックの分析には、次のコマンドを使用できます。

- **show rates**：Malicious カウンタと Legitimate カウンタの平均トラフィック レートを表示します。
- **show rates details**：すべての Guard モジュールのカウンタの平均トラフィック レートを表示します。
- **show rates history**：Malicious カウンタおよび Legitimate カウンタの平均トラフィック レートを、過去 24 時間にわたり 1 分ごとに表示します。
- **show counters**：Guard モジュールの Malicious カウンタと Legitimate カウンタを表示します。
- **show counters details**：すべての Guard モジュールのカウンタを表示します。
- **show counters history**：過去の Malicious カウンタおよび Legitimate カウンタの値を 1 分ごとに表示します。

レートの単位は bps および pps です。

（注） ゾーンのレートは、ゾーン保護をイネーブルにしている場合、またはラーニング プロセスをアクティブにしている場合にのみ使用可能です。

Guard は、トラフィックの合計を測定し、平均のトラフィック レートを計算します。値が **cleared** のレートは、ゾーンが保護されていなかった時間を示します。

カウンタの単位はパケットおよびキロビットです。カウンタは、ゾーン保護をアクティブにしたときにゼロにリセットされます。

表 11-3 に、Guard モジュールのカウンタを示します。

表 11-3　Guard モジュールのカウンタ

カウンタ	説明
Malicious	ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたカウンタとスプーフィングされたカウンタ（ゾンビ パケットも含む）の合計です。
Legitimate	Guard モジュールによってゾーンに転送された正当なトラフィック。
Received	Guard モジュールが受信し、処理したパケット。受信カウンタは、正当なカウンタと悪意のあるカウンタの合計です。
Forwarded	Guard モジュールによってゾーンに転送された正当なトラフィック。
Dropped	Guard モジュールの保護メカニズム（動的フィルタ、フレックスコンテンツ フィルタ、およびレート リミッタ モジュール）が攻撃の一部として識別し、ドロップしたパケット。
Replied	スプーフィング防止およびゾンビ防止メカニズムの一部として、信頼できるトラフィックと悪意のあるトラフィックのどちらに属するかを確認するために開始クライアントに対して応答が送信されたパケット。
Spoofed	Guard モジュールによってスプーフィングされたパケットと判断され、ゾーンに転送されなかったパケット。スプーフィングされたパケットは、応答が送信されたパケット（詳細については上の「Replied カウンタ」を参照）のうち、それに対する応答が受信されなかったものです。ゾンビ パケットは、スプーフィング パケット カウンタにも含まれています。
Invalid zone	Guard モジュールで保護されたどのゾーンも宛先としない、宛先変更されたトラフィック。この情報は、グローバル モードまたは設定モードでコマンドを入力した場合にのみ使用可能です。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# show rates
```

ゾーンのステータスの表示

特定のゾーンの概要を表示して、そのゾーンの全般的な状況と現在のステータスを知ることができます。ゾーンの概要を表示するには、ゾーン設定モードで **show** コマンドを使用します。概要には、次の情報が含まれます。

- **ゾーンのステータス**：動作状態を示します。動作状態は、保護モード、保護およびラーニングのモード、しきい値調整モード、ポリシー構築モード、または非アクティブのいずれかです。
- **ゾーンの基本設定**：動作モード（自動またはインタラクティブ）、しきい値とタイマー、IP アドレスなど、ゾーンの基本的な設定を示します。詳細については、P.6-9 の「ゾーンのアトリビュートの設定」を参照してください。
- ゾーンのフィルタ：フレックスコンテンツ　フィルタの設定も含めて、アクティブな動的フィルタおよびユーザ フィルタの設定数を示します。ゾーンがインタラクティブ保護モードの場合、概要には推奨事項の数が表示されます。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」および P.7-24 の「ユーザ フィルタの設定」を参照してください。
- **ゾーンのトラフィック　レート**：ゾーンの正当なトラフィックと悪意あるトラフィックのレートを表示します。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show
```

Guard モジュールのログの表示

Guard モジュールは、システムのアクティビティおよびイベントを自動的にログに記録します。Guard モジュールのログを表示して、Guard モジュールのアクティビティを確認および追跡できます。

表 11-4 に、イベント ログのレベルを示します。

表 11-4　イベント ログのレベル

イベントのレベル	数値コード	説明
Emergencies	0	システムが使用不能
Alerts	1	ただちに対処が必要
Critical	2	深刻な状態
Errors	3	エラー状態
Warnings	4	警告状態
Notifications	5	通常、ただし注意が必要
Informational	6	情報メッセージ
Debugging	7	デバッグ メッセージ

ログ ファイルには、すべてのログ レベル（emergencies、alerts、critical、errors、warnings、notification、informational、debugging）が表示されます。Guard モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

イベント ログは、ローカルで表示することも、リモート サーバから表示することもできます。

- イベントのリアルタイム ロギング：P.11-8 の「オンライン イベント ログの表示」を参照してください。
- ログ ファイル：P.11-11 の「ログ ファイルの表示」を参照してください。

オンライン イベント ログの表示

Guard モジュールのモニタリング メカニズムをアクティブにして、リアルタイムのイベント ログを表示できます。この設定により、Guard モジュールのイベントのオンライン ロギングを表示できます。次のコマンドを入力します。

event monitor

次の例を参考にしてください。

```
user@GUARD# event monitor
```

画面はイベントで常にアップデートされます。

（注）　モニタリング メカニズムを非アクティブにするには、**no event monitor** コマンドを使用してください。

オンライン イベント ログのエクスポート

Guard モジュールのオンライン イベント ログをエクスポートして、ログ ファイルに記録される Guard モジュールの動作を表示できます。Guard モジュールのイベントは Guard モジュールのログ ファイルにオンラインで記録されるため、リモート ホストからそのイベントを表示できます。Guard モジュールのログ ファイルは、syslog メカニズムを使用してエクスポートされます。Guard モジュールのログ ファイルは、複数の Syslog サーバにエクスポートできます。1 つのサーバがオフラインになったときに別のサーバでメッセージを受信できるように、追加のサーバを指定できます。

Guard モジュールのオンライン ログ エクスポート機能は、リモート syslog サーバを使用する場合にだけ適用できます。リモート syslog サーバが使用できない場合は、**copy log** コマンドを使用して、Guard モジュールのログ情報をファイルにエクスポートしてください。

次に、イベント ログの例を示します。

```
Sep 11 16:34:40 10.4.4.4 cm: scannet, 5 threshold-tuning-start: Zone
activation completed successfully.
```

syslog メッセージの構文は、次のとおりです。

event-date event-time Guard-IP-address protection-module zone-name event-severity-level event-type event-description

オンライン イベント ログをエクスポートするには、次の手順を実行します。

ステップ 1　（オプション）ロギング パラメータを設定します。次のコマンドを入力します。

```
logging {facility | trap}
```

表 11-5 で、**logging** コマンドのキーワードについて説明します。

表 11-5　logging コマンドのキーワード

パラメータ	説明
facility	エクスポート syslog ファシリティ。リモート syslog サーバは、ロギング ファシリティを使用してイベントをフィルタリングします。たとえば、ロギング ファシリティを使用すると、リモート ユーザは Guard モジュールのイベントを 1 つのファイルで受信し、他のネットワーク デバイスからのイベントには別のファイルを使用することができます。 使用できるファシリティは、local0 ～ local7 です。デフォルトは local4 です。
trap	リモート syslog に送信する syslog トラップの重大度。重大度のトラップ レベルには、それより高い重大度のレベルが含まれます。たとえば、トラップ レベルを **warning** に設定すると、error、critical、alerts、および emergencies も送信されます。指定できるトラップ レベルは、高い方から順に emergencies、alerts、critical、errors、warnings、notification、informational、debugging です。デフォルトは notification です。

（注） 動的フィルタの追加および削除に関するイベントを受信するには、トラップ レベルを informational に変更してください。

ステップ 2 リモート syslog サーバの IP アドレスを設定します。次のコマンドを入力します。

logging host *remote-syslog-server-ip*

または

export log *remote-syslog-server-ip*

remote-syslog-server-ip 引数には、リモート syslog サーバの IP アドレスを指定します。

ロギング メッセージを受信する syslog サーバのリストを作成するには、このコマンドを複数回入力してください。

次の例は、重大度のレベル *notification* からのトラップをファシリティ *local3* を使用して、IP アドレスが *10.0.0.191* である syslog サーバへ送信するように Guard モジュールを設定する方法を示しています。

```
user@GUARD-conf# logging facility local3
user@GUARD-conf# logging trap notifications
user@GUARD-conf# logging host 10.0.0.191
```

オンライン イベント ログのエクスポート設定を表示するには、**show logging** コマンドまたは **show log export-ip** コマンドを使用します。

ログ ファイルの表示

診断または監視のために Guard モジュールのログを表示できます。Guard モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

Guard モジュールのログを表示するには、次のコマンドを入力します。

show log

次の例を参考にしてください。

```
user@GUARD# show log
```

ゾーンのログを表示して、指定したゾーンだけに関連するイベントを確認できます。

ゾーンのログを表示するには、**show log** [*sub-zone-name*] コマンドをゾーン設定モードで使用します。*sub-zone-name* 引数には、ゾーンから作成されたサブゾーンの名前を指定します。詳細については、P.6-42 の「サブゾーンについて」を参照してください。

ログ ファイルのエクスポート

監視または診断のために、Guard モジュールのログ ファイルを FTP サーバにエクスポートできます。グローバル モードで、次のいずれかのコマンドを入力します。

- **copy** [**zone** *zone-name*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log sftp** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-6 で、**copy log ftp** コマンドの引数とキーワードについて説明します。

表 11-6　copy log ftp コマンドの引数

パラメータ	説明
zone-name	（オプション）ゾーン名。ゾーンのログ ファイルをエクスポートします。デフォルトでは、Guard モジュールのログ ファイルがエクスポートされます。
ftp	ログを FTP サーバにエクスポートします。
sftp	ログを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy log ftp 10.0.0.191 log.txt <user> <password>
```

ログ ファイルのクリア

Guard モジュールまたはゾーンのログ ファイルが大きい場合、あるいは、テストを行う予定があり、そのテスト セッションからの情報だけをログ ファイルに反映する場合は、ログ ファイルをクリアできます。

Guard モジュールまたはゾーンのログ ファイルのエントリをすべてクリアするには、設定モードまたはゾーン設定モードで次のコマンドを入力します。

clear [zone *zone-name***] log**

zone-name 引数には、ゾーン名を指定します。デフォルトでは、Guard モジュールのログ ファイルがクリアされます。**clear log** コマンドをゾーン設定モードで発行する場合、**zone** *zone-name* キーワードと引数は使用できません。ゾーン設定モードで **clear log** コマンドを使用すると、現在のゾーン ログの全エントリが消去されます。

次の例を参考にしてください。

```
user@GUARD-conf# clear log
```

ネットワーク トラフィックの監視および攻撃のシグニチャの抽出

ネットワークのトラフィック パターンを記録し、監視できます。ネットワークの動作を阻害しないタップを使用して、直接ネットワークからトラフィックを記録するように Guard モジュールを設定し、記録されたトラフィックからデータベースを作成することができます。記録されたトラフィック データベースに問い合せることにより、過去のイベントの分析や、攻撃のシグニチャの生成が可能になります。あるいは、現在のネットワークのトラフィック パターンを、トラフィックが通常状態のときに Guard モジュールによって記録された以前のトラフィック パターンと比較することが可能になります。

特定の基準を満たすトラフィックだけが Guard モジュールによって記録されるようにフィルタを設定することができます。または、すべてのトラフィック データを記録して、Guard モジュールが表示するトラフィックをフィルタリングすることもできます。

トラフィックは、Guard モジュールによって gzip 圧縮されたパケット キャプチャ（PCAP）形式で保存され、記録されたデータについて記述する Extensible Markup Language（XML）形式のファイルが付属します。

記録されたトラフィックの重要な用途は、記録された攻撃パケットのペイロードに共通のパターンまたはシグニチャが見られるかどうかを判断するというものです。Guard モジュールでは、記録されたトラフィックを分析し、シグニチャを抽出することができます。シグニチャを使用すると、そのシグニチャと一致するパケット ペイロードを含むすべてのトラフィックをブロックするようにフレックスコンテンツ フィルタを設定できます。

Guard モジュールは、次の 2 つの方法でトラフィックを記録できます。

- **自動**：Guard モジュールは常時パケットダンプ キャプチャ ファイルにトラフィック データを記録します。

  新しいパケットダンプ キャプチャ ファイルによって、以前のファイルは置き換えられます。以前のパケットダンプ キャプチャ ファイルを保存するには、FTP サーバまたは SFTP サーバにそれらのファイルをエクスポートする必要があります。
- **手動**：Guard モジュールは、パケットダンプ キャプチャ ファイルにトラフィックを記録するようにアクティブ化されたときに記録します。

以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。記録されたトラフィックを保存するには、パケットダンプ キャプチャ ファイルを FTP サーバまたは SFTP サーバにエクスポートしてから、Guard モジュールをアクティブ化して再度トラフィックを記録します。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Guard モジュールは、手動で同時に最大 4 つのゾーンについてトラフィックを記録できます。

デフォルトでは、Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

この項では、次のトピックについて取り上げます。

- Guard モジュールの設定によるトラフィックの自動記録
- Guard モジュールのアクティブ化によるトラフィックの手動記録
- Guard モジュールによるトラフィックの手動記録の停止
- 手動パケットダンプ設定の表示
- パケットダンプ キャプチャ ファイルの自動エクスポート
- パケットダンプ キャプチャ ファイルの手動エクスポート
- パケットダンプ キャプチャ ファイルのインポート
- パケットダンプ キャプチャ ファイルの表示
- パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成
- パケットダンプ キャプチャ ファイルのコピー
- パケットダンプ キャプチャ ファイルの削除

Guard モジュールの設定によるトラフィックの自動記録

Guard モジュールをアクティブにして、自動的にネットワーク トラフィックを記録することができます。このようにして、ネットワークの問題や攻撃が発生したときに分析または比較に使用可能なトラフィックの記録を入手できます。パケットダンプ キャプチャ フィルタを使用すると、指定した基準を満たすトラフィックだけが記録されるように Guard モジュールを設定できます。また、すべてのトラフィックを記録し、その記録済みのトラフィックを表示するときにパケットダンプ キャプチャ フィルタを適用することもできます。

Guard モジュールはトラフィックをキャプチャ バッファに記録します。キャプチャ バッファ サイズが 50 MB に達するか 10 分経過すると、Guard モジュールはバッファを圧縮形式でローカル ファイルに保存します。バッファは消去され、トラフィックの記録が続行されます。

Guard モジュールは、複数の自動パケットダンプ キャプチャ ファイルを保存します。記録されたトラフィックは、処理方法に基づいて分割されます。したがって、複数の自動パケットダンプ キャプチャ ファイルを 1 つの時間枠から取得できます。自動パケットダンプ キャプチャ ファイルの名前は、Guard モジュールによるトラフィックの記録時間とトラフィックの処理方法を示します。

表 11-7 で、自動パケットダンプ キャプチャ ファイル名のセクションについて説明します。

表 11-7　自動パケットダンプ キャプチャ ファイル名のセクション

セクション	説明
機能	パケットダンプ キャプチャ時に実行された Guard モジュールの機能。機能は次のいずれかになります。 • **protect**：ゾーン保護の間、Guard モジュールがトラフィックを記録。 • **learn**：ゾーンのラーニング プロセスの間、または保護およびラーニング プロセスの間、Guard モジュールがトラフィックを記録。
キャプチャ開始時刻	Guard モジュールがトラフィックの記録を開始した時刻。

表 11-7　自動パケットダンプ キャプチャ ファイル名のセクション（続き）

セクション	説明
キャプチャ終了時刻	（オプション）Guard モジュールがトラフィックの記録を完了した時刻。Guard モジュールが現在トラフィックをファイルに記録している場合、終了時刻は表示されません。
処理	Guard モジュールがトラフィックを処理した方法。アクションは次のいずれかになります。 • **forwarded**：Guard モジュールが正当なトラフィックと見なしてゾーンに転送したトラフィック • **dropped**：Guard モジュールが悪意のあるトラフィックと見なしてドロップしたトラフィック • **replied**：パケットが正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、Guard モジュールがスプーフィング防止メカニズムまたはゾンビ防止メカニズムによる処理の一環として、開始側のクライアントに応答を送信したトラフィック

Guard モジュールは、ラーニング プロセスからパケットダンプ キャプチャ ファイルを 1 つ保存します。ゾーン保護の間、Guard モジュールは次のパケットダンプ キャプチャ ファイルを保存します。

- 直前 10 分間のトラフィックのパケットダンプ キャプチャ ファイル 1 つ
- 現在のトラフィックのパケットダンプ キャプチャ ファイル 1 つ

ゾーン保護をアクティブにするか、または自動的にネットワーク トラフィックが記録されるように Guard モジュールをアクティブにすると、保護プロセスで記録された以前のパケットダンプ キャプチャ ファイルはすべて Guard モジュールによって消去され、新しいファイルが作成されます。

自動的にネットワーク トラフィックを記録するように Guard モジュールを設定するには、次の手順を実行します。

ステップ 1　ゾーン トラフィックを自動的に記録するように Guard モジュールを設定します。ゾーン設定モードで次のコマンドを入力します。

```
packet-dump auto-capture
```

ステップ 2　（オプション）パケットダンプ　キャプチャ　データベースを作成するには、FTP サーバまたは SFTP サーバにパケットダンプ キャプチャ ファイルをエクスポートします。P.11-22 の「パケットダンプ キャプチャ ファイルの自動エクスポート」を参照してください。

以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。パケットダンプ キャプチャ データベースを作成するには、パケットダンプ キャプチャ ファイルをエクスポートする必要があります。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# packet-dump auto-capture
```

Guard モジュールでゾーンのトラフィック データを自動的にキャプチャしないようにするには、**no packet-dump auto-capture** コマンドを使用します。

現在のパケットダンプ設定を表示するには、**show packet-dump** コマンドを使用します。

Guard モジュールのアクティブ化によるトラフィックの手動記録

Guard モジュールをアクティブにして、トラフィックの記録を開始できます。このようにして、特定期間のトラフィックを記録したり、あるいは Guard モジュールがトラフィックの記録に使用する基準を変更することができます。

指定されたパケット数を記録するか、ラーニング プロセスまたはゾーン保護が終了すると、Guard モジュールはトラフィックの記録を停止し、手動パケットダンプ キャプチャをファイルに保存します。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Guard モジュールは、同時に 10 ゾーンまで手動パケットダンプ キャプチャを記録できます。

手動パケットダンプ キャプチャをアクティブにするには、ゾーン設定モードで次のコマンドを入力します。

packet-dump capture [**view**] *capture-name pdump-rate pdump-count* {**all** | **dropped** | **forwarded** | **replied**} [***tcpdump-expression***]

（注） トラフィックをキャプチャする間は、CLI セッションが停止します。キャプチャの実行中に作業を続行するには、Guard モジュールとの追加のセッションを確立してください。

表 11-8 で、**packet-dump** コマンドの引数とキーワードについて説明します。

表 11-8　packet-dump コマンドの引数とキーワード

パラメータ	説明
view	（オプション）Guard モジュールが記録しているトラフィックをリアルタイムに表示します。
capture-name	パケットダンプ キャプチャ ファイルの名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。

表 11-8　packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
pdump-rate	サンプル レート（pps）。1 ～ 10000 の値を入力します。 **（注）** Guard モジュールは、すべての同時手動キャプチャに対する最大の累積パケットダンプ キャプチャレートとして、10000 パケット / 秒をサポートします。 高いサンプル レート値を設定したパケットダンプ キャプチャは、多くのリソースを消費します。パフォーマンスに悪影響を与える可能性があるので、高いレート値を設定するときは注意してください。
pdump-count	記録対象のパケット数。Guard モジュールは、指定されたパケット数の記録を終了すると、手動パケットダンプ キャプチャ バッファをファイルに保存します。1 ～ 5000 の整数を入力します。
all	すべてのトラフィックをキャプチャします。
dropped	Guard モジュールがドロップしたトラフィックだけをキャプチャします。
forwarded	Guard モジュールがゾーンに転送した正当なトラフィックだけをキャプチャします。
replied	検証の試行で Guard モジュールのスプーフィング防止メカニズムおよびゾンビ防止メカニズムが送信元に返送したトラフィックだけをキャプチャします。
tcpdump-expression	（オプション）記録対象のトラフィックを指定するために適用するフィルタ。Guard モジュールはフィルタの式に適合するトラフィックだけをキャプチャします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# packet-dump capture view 10 1000 all
```

Guard モジュールによるトラフィックの手動記録の停止

Guard モジュールは、手動パケットダンプ キャプチャをアクティブにしたときに指定したパケット数を記録すると、キャプチャを停止します。しかし、指定したパケット数が Guard モジュールによって記録される前に、手動パケットダンプ キャプチャを停止することができます。

Guard モジュールによるトラフィックの手動記録を停止するには、次のいずれかのアクションを実行します。

- 開かれている CLI セッションで Ctrl+C を押す。
- 新しい CLI セッションを開き、関連するゾーン設定モードで次のコマンドを入力する。

  no packet-dump capture *capture-name*

  capture-name 引数には、停止するキャプチャの名前を指定します。

Guard モジュールは、パケットダンプ キャプチャ ファイルを保存します。

手動パケットダンプ設定の表示

Guard モジュールによって手動パケットダンプ キャプチャ ファイル用に割り当てられたディスク スペースの現在の容量を表示するには、設定モードまたはグローバル モードで **show packet-dump** コマンドを使用します。Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 1 ブロックのディスク スペースを割り当てています。

次の例を参考にしてください。

```
user@GUARD-conf# show packet-dump
```

表 11-9 で、**show packet-dump** コマンド出力のフィールドについて説明します。

表 11-9　手動の show packet-dump コマンド出力のフィールドの説明

フィールド	説明
Allocated disk-space	Guard モジュールによって、すべてのゾーンの手動パケットダンプ キャプチャ用に割り当てられたディスク スペースの合計量を指定します（MB 単位）。
Occupied disk-space	割り当てられたディスク スペースのうち、すべてのゾーンからの手動パケット ダンプ ファイルによって消費されたパーセンテージを示します。

パケットダンプ キャプチャ ファイルの自動エクスポート

パケットダンプ キャプチャ ファイルを自動的に FTP サーバまたは SFTP サーバにエクスポートするように Guard モジュールを設定できます。自動エクスポート機能をイネーブルにすると、Guard モジュールはパケットダンプ バッファの内容をローカル ファイルに保存するたびに、パケットダンプ キャプチャ ファイルをエクスポートします。パケットダンプ キャプチャ ファイルは gzip 圧縮された PCAP 形式でエクスポートされ、記録されたデータについて記述する XML 形式のファイルが付属します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。

パケットダンプ キャプチャ ファイルを自動的にエクスポートするには、設定モードで次のいずれかのコマンドを入力します。

- **export packet-dump ftp** *server full-file-name* [*login* [*password*]]
- **export packet-dump sftp** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-10 で、**export packet-dump** コマンドの引数について説明します。

表 11-10　export packet-dump コマンドの引数

パラメータ	説明
ftp	パケットダンプ キャプチャ ファイルを FTP サーバにエクスポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	Guard モジュールによるパケットダンプ キャプチャ ファイルの保存先の完全パス名。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例は、IP アドレスが *10.0.0.191* の FTP サーバにパケットダンプ キャプチャ ファイルを自動的にエクスポートする方法を示しています。

```
user@GUARD# export packet-dump ftp 10.0.0.191 /root/captures/ <user> <password>
```

パケットダンプ キャプチャ ファイルの手動エクスポート

パケットダンプ キャプチャ ファイルを FTP サーバに手動でエクスポートできます。パケットダンプ キャプチャ ファイルを 1 つエクスポートすることも、特定のゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートすることもできます。Guard モジュールによって、パケットダンプ キャプチャ ファイルは gzip 圧縮された PCAP 形式でエクスポートされ、記録されたデータについて記述する XML ファイルが付属します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。

パケットダンプ キャプチャ ファイルを FTP サーバに手動でエクスポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **ftp** *server full-file-name* [*login* [*password*]]
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **sftp** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-11 で、**copy zone packet-dump** コマンドの引数とキーワードについて説明します。

表 11-11　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートします。詳細については、P.11-27 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。
ftp	パケットダンプ キャプチャ ファイルを FTP サーバにエクスポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	Guard モジュールによるパケットダンプ キャプチャ ファイルの保存先の完全パス名。

表 11-11　copy zone packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy zone scannet packet-dump captures ftp 10.0.0.191 <user> <password>
```

パケットダンプ キャプチャ ファイルのインポート

パケットダンプ キャプチャ ファイルを FTP サーバから Guard モジュールにインポートできます。このようにして、過去のイベントを分析したり、現在のネットワークのトラフィック パターンを、Guard モジュールによってトラフィックが通常状態のときに記録された以前のトラフィック パターンと比較することができます。Guard モジュールは、XML 形式と PCAP 形式のパケットダンプ キャプチャ ファイルをどちらもインポートします。

パケットダンプ キャプチャ ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy ftp zone** *zone-name* **packet-dump captures** *server full-file-name* [*login* [*password*]]
- **copy sftp zone** *zone-name* **packet-dump captures** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-12 で、**copy zone packet-dump** コマンドの引数について説明します。

表 11-12　copy zone packet-dump コマンドの引数

パラメータ	説明
zone-name	パケットダンプ キャプチャ ファイルをインポートする既存のゾーンの名前。
ftp	パケットダンプ キャプチャ ファイルを FTP サーバからインポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP サーバからインポートします。
server	サーバの IP アドレス。
full-file-name	インポート対象のファイルの完全なパスとファイル名。ファイル拡張子は除きます。パスを指定しない場合、サーバはユーザのホーム ディレクトリからファイルをコピーします。 **（注）** ファイル拡張子を指定しないでください。指定すると、インポート プロセスは失敗します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy ftp zone scannet packet-dump captures 10.0.0.191
capture-1 <user> <password>
```

パケットダンプ キャプチャ ファイルの表示

パケットダンプ キャプチャ ファイルのリスト、または 1 つのパケットダンプ キャプチャ ファイルの内容を表示できます。デフォルトでは、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルすべてのリストを表示します。

パケットダンプ キャプチャ ファイルを表示するには、ゾーン設定モードで次のコマンドを入力します。

show packet-dump captures [*capture-name* [*tcpdump-expression*]]

表 11-13 に、**show packet-dump captures** コマンドの引数を示します。

表 11-13　show packet-dump captures コマンドの引数

パラメータ	説明
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルすべてのリストを表示します。コマンド出力のフィールド説明については、表 11-14 を参照してください。 パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはファイルを TCPDump 形式で表示します。
tcpdump-expression	（オプション）パケットダンプ キャプチャ ファイルを表示するときに Guard モジュールが使用するフィルタ。Guard モジュールは、フィルタ基準に一致する一部のパケットダンプ キャプチャ ファイルだけを表示します。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show packet-dump captures
```

表 11-14 で、**show packet-dump captures** コマンド出力のフィールドについて説明します。

表 11-14　show packet-dump captures コマンド出力のフィールドの説明

フィールド	説明
Capture -name	パケットダンプ キャプチャ ファイルの名前。自動パケットダンプ キャプチャ ファイル名については、表 11-7 を参照してください。
Size (MB)	パケットダンプ キャプチャ ファイルのサイズ（MB）。
Filter	Guard モジュールがトラフィックの記録時に使用したユーザ定義のフィルタ。このフィルタは TCPDump 形式です。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成

攻撃シグニチャは、攻撃パケットのペイロードに見られる共通パターンを記述するものです。Guard モジュールをアクティブにして異常なトラフィックのシグニチャを生成し、この情報を使用してタイプが同じ将来の攻撃をすばやく識別することができます。この機能を使用すると、アンチウィルス ソフトウェアのメーカーやメーリング リストなどからシグニチャが発行される前であっても、新しい DDoS 攻撃やインターネット ワームを検出することができます。

Guard モジュールは、フレックスコンテンツ フィルタのパターン式の構文を使用して攻撃のシグニチャを生成します。このシグニチャをフレックスコンテンツ フィルタのパターンで使用して、異常なトラフィックをフィルタリングして排除できます。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」を参照してください。

参照用として、トラフィックが通常状態（平時）のときに Guard モジュールによって記録された追加のパケットダンプ キャプチャ ファイルを指定できます。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Guard モジュールは異常なトラフィックからシグニチャを生成し、トラフィックが通常状態のと

きに記録されたトラフィックの中に、シグニチャが存在している時間の割合を特定します。正常のトラフィック状態で記録されたトラフィックに攻撃シグニチャが高い確率で出現しても、攻撃パターンを意味するとは限りません。

攻撃のシグニチャを生成するには、次の手順を実行します。

ステップ 1　Guard　モジュールをアクティブにして、攻撃進行中のトラフィックを記録します。**packet-dump capture** コマンドを使用します（P.11-18 の「Guard モジュールのアクティブ化によるトラフィックの手動記録」を参照）。

ステップ 2　攻撃進行中に Guard モジュールが記録したパケットダンプ キャプチャ ファイルを識別します。**show packet-dump captures** コマンドを使用して、パケットダンプ キャプチャ ファイルのリストを表示します。詳細については、P.11-27 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。

ステップ 3　Guard モジュールをアクティブにして、攻撃されたトラフィックのシグニチャを生成します。ゾーン設定モードで次のコマンドを入力します。

```
show packet-dump signatures capture-name [reference-capture-name]
```

表 11-15 に、**show packet-dump signatures** コマンドの引数を示します。

表 11-15　show packet-dump signatures コマンドの引数

パラメータ	説明
capture-name	シグニチャの生成元である既存のパケットダンプ キャプチャ ファイルの名前。
reference-capture-name	（オプション）トラフィックが通常状態のときに Guard モジュールによって記録された既存のパケットダンプ キャプチャ ファイルの名前。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Guard モジュールは参照用のパケットダンプ キャプチャ ファイルの中に、シグニチャが存在している時間の割合を表示します。

表 11-16 で、**show packet-dump signatures** コマンド出力のフィールドについて説明します。

表 11-16　show packet-dump signatures コマンド出力のフィールドの説明

フィールド	説明
Start Offset	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット（バイト単位）。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *start-offset* 引数にコピーします。
End Offset	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット（バイト単位）。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *end-offset* 引数にコピーします。
Pattern	Guard モジュールが生成したシグニチャ。Guard モジュールは、フレックスコンテンツ フィルタのパターン式の構文を使用してシグニチャを生成します。詳細については、P.7-16 の「パターン式の構文について」を参照してください。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーできます。
Percentage	シグニチャが *reference-capture-name* ファイルに存在する時間の割合。

次の例は、手動パケットダンプ キャプチャ ファイルからシグニチャを生成する方法を示しています。

```
user@GUARD-conf-zone-scannet# show packet-dump signatures PDumpCapture
```

パケットダンプ キャプチャ ファイルのコピー

1 つのパケットダンプ キャプチャ ファイル、または 1 つのファイルの一部を、新しい名前でコピーできます。

Guard モジュールは、既存の自動パケットダンプ キャプチャ ファイルを新しいファイルで上書きします。自動パケットダンプ キャプチャ ファイルをコピーする場合、Guard モジュールはそのファイルを手動パケットダンプ キャプチャ ファイルとして保存し、新しいファイルで上書きしません。つまり、ディスク スペースを解放するには、そのファイルを手動で削除する必要があります。

手動パケットダンプ キャプチャ ファイルをコピーする場合も、Guard モジュールは元のファイルのコピーを保存します。ディスク スペースを解放する必要がある場合は、そのコピーを手動で削除します。

詳細については、P.11-32 の「パケットダンプ キャプチャ ファイルの削除」を参照してください。

パケットダンプ キャプチャ ファイルをコピーするには、設定モードで次のコマンドを入力します。

copy zone *zone-name* **packet-dump captures** ***capture-name*** [***tcpdump-expression***] ***new-name***

表 11-17 に、**copy packet-dump captures** コマンドの引数を示します。

表 11-17　copy packet-dump captures コマンドの引数

パラメータ	説明
zone-name	コピー対象のパケットダンプ キャプチャ ファイルがある既存のゾーンの名前。
capture-name	既存のパケットダンプ キャプチャ ファイルの名前。
tcpdump-expression	（オプション）パケットダンプ キャプチャ ファイルをコピーするときに Guard モジュールが使用するフィルタ。Guard モジュールは、フィルタ基準に一致する一部のパケットダンプ キャプチャ ファイルだけをコピーします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

表 11-17　copy packet-dump captures コマンドの引数（続き）

パラメータ	説明
new-name	新しいパケットダンプ キャプチャ ファイルの名前。この名前は 1 ～ 63 文字の英数字の文字列です。アンダースコアを含めることができますが、スペースを含めることはできません。

次の例を参考にしてください。

```
user@GUARD-conf# copy zone scannet capture-1 "tcp and dst port 80 and
not src port 1000" capture-2
```

パケットダンプ キャプチャ ファイルの削除

デフォルトでは、Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

手動パケットダンプ キャプチャ ファイルは、ゾーンごとに 1 つだけ保存でき、10 個を超えるパケットダンプ キャプチャ ファイルを Guard モジュールに置くことはできません。新しい手動パケットダンプ キャプチャ ファイルのためのスペースを解放するには、古いファイルを削除する必要があります。

自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルを削除するには、次のいずれかのコマンドを入力します。

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*}—In configuration mode
- **clear packet-dump captures** {***** | *name*}—In zone configuration mode

表 11-18 に、**clear packet-dump** コマンドの引数を示します。

表 11-18　clear packet-dump コマンドの引数

パラメータ	説明
zone-name	既存のゾーンの名前。
*	すべてのパケットダンプ キャプチャ ファイルを消去します。
name	消去対象のパケットダンプ キャプチャ ファイルの名前。

次の例は、すべての手動パケットダンプ キャプチャ ファイルを消去する方法を示しています。

```
user@GUARD-conf# clear packet-dump captures *
```

一般的な診断データの表示

Guard モジュールの一般的な診断データを表示できます。

一般的な診断データを表示するには、次のコマンドを入力します。

show diagnostic-info

診断データは、次の情報で構成されます。

- **Line Card Number**：Guard の識別子ストリング。
- **Number of Pentium-class Processors**：Guard モジュールのプロセッサの番号。Guard モジュールはプロセッサ 1 をサポートします。
- **BIOS Vendor**：Guard の BIOS のベンダー。
- **BIOS Version**：Guard の BIOS バージョン。
- **Total available memory**：Guard で使用可能なメモリの合計量。
- **Size of compact flash**：Guard のコンパクト フラッシュのサイズ。
- **Slot Num**：モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
- **CFE version**：CFE のバージョン番号。

（注）　CFE のバージョンを変更するには、新しいフラッシュ バージョンをインストールする必要があります。CFE の新しいバージョンを焼き付けるには、**flash-burn** コマンドを使用してください。詳細については、P.12-8 の「Guard モジュールのバージョンのアップグレード」を参照してください。

- **Recognition Average Sample Loss**：認識モジュールの、計算されたパケット サンプル損失。
- **Forward failures (no resources)**：システム リソースが不足しているために転送されなかったパケット数。

（注）　**Recognition Average Sample Loss** または **Forward failures** の値が大きいと、Guard モジュールはトラフィックで過負荷の状態になることを示します。複数の Guard モジュールを負荷分散型構成にインストールすることをお勧めします。

メモリ消費量の表示

Guard モジュールのメモリ消費量を表示できます。Guard モジュールは、メモリ使用量を KB 単位で表示します。さらに、Guard モジュールは、認識保護モジュールが使用しているメモリのパーセンテージも表示します。認識保護モジュールのメモリ使用率は、アクティブなゾーンの数、および各ゾーンが監視するサービスの数に影響されます。

（注） 認識保護モジュールのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

次のコマンドを入力します。

show memory

次の例を参考にしてください。

```
user@GUARD# show memory
              total    used    free    shared   buffers   cached
  In KBytes:  2065188  146260  1918928    0     2360      69232

  Recognition Used Memory: 0.3%
```

（注） Guard モジュールの空きメモリの合計量は、**free** メモリと **cached** メモリの合計です。

CPU 使用率の表示

現在の CPU 使用率（パーセンテージ）を表示できます。Guard モジュールは、ユーザ モード、システム モード、ナイス値が負のタスク、およびアイドル状態の CPU 時間のパーセンテージを表示します。ナイス値が負のタスクは、システム時間およびユーザ時間にもカウントされるため、CPU 使用率の合計が 100% を超えることがあります。

次のコマンドを入力します。

show cpu

次の例を参考にしてください。

```
user@GUARD# show cpu
Host CPU:  0.0% user,  0.1% system,  0.0% nice, 99.0% idle
```

ARP キャッシュの操作

ARP キャッシュを表示または操作して、アドレス マッピング エントリを消去または手動で定義できます。次のいずれかのコマンドを入力します。

arp [**-evn**] [**-H** *type*] [**-i** *if*] **-a** [*hostname*]

arp [**-v**] [**-i** *if*] **-d** *hostname* [**pub**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**netmask** *nm*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if*] **-Ds** *hostname* ifa [**netmask** *nm*] **pub**

arp [**-vnD**] [**-H** *type*] [**-i** *if*] **-f** [*filename*]

表 11-19 で、**arp** コマンドの引数とキーワードについて説明します。

表 11-19　arp コマンドの引数とキーワード

パラメータ	説明
-v、--verbose	出力を詳細に表示します。
-n、--numeric	数値アドレスを表示します。
-H *type*、**--hw-type** *type*、**-t** *type*	Guard モジュールがチェックするエントリのクラスを指定します。このパラメータのデフォルト値は、ether（IEEE　802.3 10Mbps イーサネットに対応するハードウェア コード 0x01）です。
-a [*hostname*]、**--display** [*hostname*]	指定したホストのエントリを代替（BSD）形式で表示します。デフォルトでは、すべてのエントリが表示されます。
-d *hostname*、**--delete** *hostname*	指定したホストのエントリを削除します。
-D、**--use-device**	インターフェイス ifa のハードウェア アドレスを使用します。
-e	エントリをデフォルトの形式で表示します。

表 11-19　arp コマンドの引数とキーワード（続き）

パラメータ	説明
-i *If*、**--device** *If*	インターフェイスを指定します。ARP キャッシュをダンプすると、指定したインターフェイスに一致するエントリだけが出力されます。永続的または一時的な ARP エントリを設定する場合、このインターフェイスがそのエントリに関連付けられます。このオプションを使用しない場合、Guard モジュールはルーティング テーブルに基づいてインターフェイスを推測します。pub エントリの場合、これは Guard モジュールが ARP 要求に応えるインターフェイスで、IP データグラムのルーティング先のインターフェイスとは異なっている必要があります。
-s *hostname hw_addr*、*--***set** *hostname*	ハードウェア アドレスを *hw_addr* クラスに設定して、ホスト *hostname* の ARP アドレス マッピング エントリを作成します。ほとんどのクラスでは、通常の表現を使用できます。
-f *filename*、**--file** *filename*	ARP アドレス マッピング エントリを作成します。情報は、ファイル *filename* から取得されます。ファイル形式は、ホスト名とハードウェア アドレスが空白で区切られた ASCII テキスト行です。pub、temp、および netmask フラグを使用することもできます。ホスト名を入力するどの場所にも、ドット区切り 10 進表記で IP アドレスを入力できます。

注意　Guard モジュールの ARP キャッシュを設定するには、Guard モジュール システムとネットワークの知識が必要です。

次の例を参考にしてください。

```
user@GUARD# arp -e

Address         HWtype  HWaddress           Flags Mask  Iface
10.10.1.254     ether   00:02:B3:C0:61:67   C           eth1
10.10.8.11      ether   00:02:B3:45:B9:F1   C           eth1
10.10.8.253     ether   00:D0:B7:46:72:37   C           eth1
10.10.10.54     ether   00:03:47:A6:44:CA   C           eth1
```

netstat の使用

ホスト ネットワーク接続、ルーティング テーブル、インターフェイス統計情報、マスカレード接続、およびマルチキャスト メンバシップを表示して、ネットワークの問題をデバッグできます。次のいずれかのコマンドを入力します。

netstat [*address_family_options*] [--**tcp**|-**t**] [--**udp**|-**u**] [--**raw**|-**w**] [--**listening**|-**l**] [--**all**|-**a**] [--**numeric**|-**n**]
[--**numeric-hosts**][--**numeric-ports**][--**numeric-ports**] [--**symbolic**|-**N**]
[--**extend**|-**e**[--**extend**|-**e**]][--**timers**|-**o**] [--**program**|-**p**] [--**verbose**|-**v**]
[--**continuous**|-**c**] [*delay*]

netstat {--**route**|-**r**} [*address_family_options*] [--**extend**|-**e**[--**extend**|-**e**]]
[--**verbose**|-**v**] [--**numeric**|-**n**]
[--**numeric-hosts**][--**numeric-ports**][--**numeric-ports**] [--**continuous**|-**c**]
[*delay*]

netstat {--**interfaces**|-**i**} [*iface*] [--**all**|-**a**] [--**extend**|-**e**[--**extend**|-**e**]] [--**verbose**|-**v**]
[--**program**|-**p**] [--**numeric**|-**n**]
[--**numeric-hosts**][--**numeric-ports**][--**numeric-ports**] [--**continuous**|-**c**]
[*delay*]

netstat {--**groups**|-**g**} [--**numeric**|-**n**] [--**numeric-hosts**][--**numeric-ports**][--**numeric-ports**] [--**continuous**|-**c**] [*delay*]

netstat {--**masquerade**|-**M**} [--**extend**|-**e**] [--**numeric**|-**n**] [--**numeric-hosts**][--**numeric-ports**][--**numeric-ports**] [--**continuous**|-**c**] [*delay*]

netstat {--**statistics**|-**s**} [--**tcp**|-**t**] [--**udp**|-**u**] [--**raw**|-**w**] [*delay*]

netstat {--**version**|-**V**}

netstat {--**help**|-**h**}

（注） アドレス ファミリを指定しない場合、Guard モジュールは設定されているすべてのアドレス ファミリのアクティブなソケットを表示します。

表 11-20 で、**netstat** コマンドの引数とキーワードについて説明します。

表 11-20　netstat コマンドの引数とキーワード

パラメータ	説明
address_family_options	[--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]][--unix|-x][--inet|--ip] [--ax25] [--ipx] [--netrom] [--ddp]
--route、-r	Guard モジュールのルーティング テーブルを表示します。
--groups、-g	IPv4 および IPv6 のマルチキャスト グループ メンバシップ情報を表示します。
--interface、-i *iface*	すべてのネットワーク インターフェイスまたはインターフェイス *iface* のテーブルを表示します。
--masquerade、-M	マスカレード接続のリストを表示します。
--statistics、-s	各プロトコルのサマリー統計情報を表示します。
-v、--verbose	出力を詳細に表示します。
-n、--numeric	数値アドレスを表示します。
--numeric-hosts	数値ホスト アドレスを表示します。これは、ポート名およびユーザ名の解決に影響を及ぼしません。
--numeric-ports	数値ポート番号を表示します。これは、ホスト名およびユーザ名の解決に影響を及ぼしません。
--numeric-users	数値ユーザ ID を表示します。これは、ホスト名およびポート名の解決に影響を及ぼしません。
--protocol、-A *family*	接続を表示するアドレス低レベル プロトコル（ファミリ）を指定するカンマ区切りリスト。アドレス ファミリ inet には、raw、udp、および tcp プロトコル ソケットが含まれます。
-c、--continuous	選択した情報を 1 秒ごとに継続的に表示します。
-e、--extend	追加情報を表示します。最も詳しい情報を表示するには、このオプションを 2 回使用します。
-o、--timers	ネットワーキング タイマーに関連する情報を表示します。
-p、--program	各ソケットが属するプログラムの PID および名前を表示します。

表 11-20　netstat コマンドの引数とキーワード（続き）

パラメータ	説明
-l、--listening	リスニング ソケットだけを表示します。デフォルトでは、リスニング ソケットは省略されます。
-a、--all	リスニング ソケットと非リスニング ソケットの両方を表示します。
-F	FIB からのルーティング情報を表示します。
-C	ルート キャッシュからのルーティング情報を表示します。
delay	*delay* 秒ごとに、netstat が統計情報からの出力を繰り返します。

1 つのコマンドに最大 13 の引数とキーワードを入力できます。

次の例を参考にしてください。

```
user@GUARD# netstat -v
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address         State
tcp        0      0 localhost:1111  localhost:32777    ESTABLISHED
tcp        0      0 localhost:8200  localhost:32772    ESTABLISHED
.
.
.
tcp        0      0 localhost:33464 localhost:8200     TIME_WAIT
tcp        1      0 localhost:1113  localhost:33194    CLOSE_WAIT
.
.
.
Active UNIX domain sockets (w/o servers)
unix  2      [ ]         STREAM     CONNECTED     928
unix  3      [ ]         STREAM     CONNECTED     890  /tmp/.zserv
.
.
.
user@GUARD#
```

traceroute の使用

パケットがネットワーク ホストに到達するまでのルートを出力して、ネットワークの問題をデバッグできます。次のコマンドを入力します。

traceroute *ip-address* [**-F**] [**-f** *first_ttl*] [**-g** *gateway*] [**-i** *iface*] [**-m** *max_ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] [*packetlen*]

（注） **traceroute** コマンドでは IP アドレスだけが表示され、名前は表示されません。

表 11-21 で、**traceroute** コマンドの引数とキーワードについて説明します。

表 11-21　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	どの IP アドレスへのルートをトレースするか。
-f *first_ttl*	最初の発信プローブ パケットで使用される最初の Time-To-Live（TTL; 存続可能時間）を設定します。
-F	*don't fragment* ビットを設定します。
-g *gateway*	ルース ソース ルート ゲートウェイを指定します（最大 8 個）。
-i *iface*	発信プローブ パケットの送信元 IP アドレスを取得するネットワーク インターフェイスを指定します。これは通常、マルチホーム ホストで役立ちます。
-m *max_ttl*	発信プローブ パケットで使用される最大存続可能時間（最大ホップ数）を設定します。デフォルトは 30 ホップです。
-p *port*	プローブで使用されるベース UDP ポート番号を設定します。デフォルトは 33434 です。
packetlen	プローブのパケットの長さを設定します。
-s *src_addr*	IP アドレス *src_addr* を発信プローブ パケットで送信元 IP アドレスとして設定します。

表 11-21　traceroute コマンドの引数とキーワード（続き）

パラメータ	説明
-t *tos*	プローブ パケットのサービス タイプを、*tos* の値に設定します。デフォルトはゼロです。
-w *waittime*	プローブに対する応答を待つ時間（秒）を設定します。デフォルトは 5 秒です。

次の例を参考にしてください。

```
user@GUARD# traceroute 10.10.10.34
traceroute to 10.10.10.34 (10.10.10.34), 30 hops max, 38 byte packets
 1 10.10.10.34 (10.10.10.34) 0.577 ms  0.203 ms  0.149 ms
```

ping の使用

ネットワーク ホストに ICMP ECHO_REQUEST パケットを送信して、接続性を確認できます。次のコマンドを入力します。

ping *ip-address* [**-c** *count*] [**-i** *interval*] [**-l** *preload*] [**-s** *packetsize*] [**-t** *ttl*] [**-w** *deadline*] [**-F** *flowlabel*] [**-I** *interface*] **[-Q** *tos*] [**-T** *timestamp option*] [**-W** *timeout*]

表 11-22 で、**ping** コマンドの引数とキーワードについて説明します。

表 11-22　ping コマンドの引数とキーワード

パラメータ	説明
ip-address	宛先 IP アドレス。
-c *count*	*count* 個の ECHO_REQUEST パケットを送信します。deadline オプションが指定されている場合、ping はタイムアウトになるまでこの数の ECHO_REPLY パケットを待ちます。
-F *flow label*	エコー要求パケットに 20 ビットのフロー ラベルを割り当てて設定します（ping6 のみ）。値がゼロの場合は、ランダムなフロー ラベルが使用されます。
-i *interval*	パケットの送信間隔を *interval* 秒に設定します。デフォルトでは、1 秒に設定されます。
-I *interface*	送信元 IP アドレスを、指定したインターフェイス アドレスに設定します。
-l *preload*	応答を待たずに *preload* 個のパケットを送信します。
-Q *tos*	ICMP データグラムに Quality of Service（QoS）関連のビットを設定します。
-s *packetsize*	送信するデータ バイト数を指定します。デフォルトは 56 です。
-t ttl	IP の TTL を設定します。
-T *timestamp option*	特別な IP タイムスタンプ オプションを設定します。

表 11-22　ping コマンドの引数とキーワード（続き）

パラメータ	説明
-w *deadline*	送受信されたパケット数に関係なく ping が終了するまでのタイムアウト（秒）を指定します。
-W *timeout*	応答を待つ時間（秒）。

1 つのコマンドに最大 10 の引数とキーワードを入力できます。

次の例を参考にしてください。

```
user@GUARD# ping 10.10.10.30 -n 1
```

デバッグ情報の取得

Guard モジュールに動作上の問題が発生した場合は、シスコのテクニカルサポートがお客様に Guard モジュールの内部デバッグ情報のコピーを送信するようお願いすることがあります。Guard モジュールのデバッグ コア ファイルには、Guard モジュールの誤動作についてトラブルシューティングを行うための情報が含まれています。このファイルの出力は暗号化されており、Cisco TAC の担当者のみが使用するよう意図されています。

デバッグ情報を FTP サーバに抽出するには、次の手順を実行します。

ステップ 1　Guard モジュール のログ ファイルを表示します。詳細については、P.11-11 の「ログ ファイルの表示」を参照してください。

ステップ 2　デバッグ情報を収集する時刻を特定します。問題があることを示している最初のログ メッセージを識別します。

ステップ 3　デバッグ情報を FTP サーバに抽出します。次のコマンドを入力します。

```
copy debug-core time ftp server full-file-name [login [password]]
```

表 11-23 で、**copy debug-core** コマンドの引数について説明します。

表 11-23　copy debug-core コマンドの引数

パラメータ	説明
time	デバッグ情報が必要となった原因のイベントの時刻。時刻の文字列では、*MMDDhhmm*[[*CC*]*YY*][*.ss*] という形式を使用します。 • *MM*：月（数値）。 • *DD*：日。 • *hh*：時（24 時間表記）。 • *mm*：分。 • *CC*：（オプション）年の最初の 2 桁（たとえば **20**05）。 • *YY*：（オプション）年の最後の 2 桁（たとえば 20**05**）。 • *.ss*：（オプション）秒（小数点が必要）。
server	FTP サーバの IP アドレス。
full-file-name	バージョン ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	（オプション）FTP サーバのログイン名。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy debug-core 11090645 ftp 10.0.0.191
/home/debug/debug-file <user> <password>
```

Guard モジュールの自己保護設定の表示

独立した IP アドレスを持つネットワーク要素としての Guard モジュールは、潜在的な DDoS 攻撃の危険にさらされています。デフォルトの設定では、このような攻撃に対する保護が提供されます。ユーザは、この自己防衛保護設定にアクセスし、変更することができます。

注意　Guard　モジュールの自己防衛保護のデフォルト設定は変更しないことを強くお勧めします。不要な設定の結果として、Guard モジュールの自己保護機能に大きな支障をきたす場合があります。

Guard モジュールの自己防衛保護設定を変更するには、自己保護設定モードに入る必要があります。

自己保護設定モードに入るには、設定モードで次のコマンドを入力します。

self-protection

Guard モジュールの自己防衛保護に使用できるコマンドのセットは、通常のゾーンで使用できるものと同じです。ゾーンの設定の詳細については、第 6 章「ゾーンの設定」、第 7 章「ゾーンのフィルタの設定」、第 8 章「ポリシー テンプレートとポリシーの設定」、および第 9 章「インタラクティブ保護モード」を参照してください。

Guard モジュールの自己保護設定ファイルを表示するには、**show running-config** コマンドを使用します。詳細については、「Guard モジュールの設定の表示」を参照してください。

フレックスコンテンツ フィルタのデフォルト設定

Guard モジュールのフレックスコンテンツ フィルタは、明示的な指定がない限り、デフォルトですべてのトラフィック フローをブロック（ドロップ）するように設定されています。表 11-24 に、Guard モジュールが適切に機能するために必要な通信を可能にするためのフレックスコンテンツ フィルタのデフォルト設定を示します。

表 11-24　フレックスコンテンツ フィルタのデフォルト設定

サービス	IP プロトコル	送信元ポート	宛先ポート	同期の許可
ftp-control	6	21	*	no
ftp-data	6	20	*	yes
tacacs	6	49	*	yes
ssh	6	22	*	no
ssh	6	*	22	yes
https	6	*	443	yes
icmp	1	*	*	—
snmp	17	*	161	—
ssl	6	*	3220	no
ssl	6	3220	*	yes

フレックスコンテンツ フィルタのデフォルト設定は、次の内容で構成されます。

- Guard モジュールによって開始される FTP サーバとの FTP 通信をイネーブル化し、送信元ポート 21 で着信 FTP 制御 SYN パケットをブロックする。
- TACACS+ サーバとの TACACS 通信をイネーブル化し、送信元ポート 49 からの着信 SYN パケットをブロックする。この設定により、認証、認可、アカウンティングのための TACACS+ サーバとの通信が可能になります。
- 着信および発信 SSH 通信をイネーブルにする。
- 着信 HTTPS 通信をイネーブルにする。
- ICMP 通信をイネーブルにする。
- SNMP 通信をイネーブルにする。
- SSL 通信をイネーブルにする。

CHAPTER 12

メンテナンス タスクの実行

この章では、Cisco Anomaly Guard Module（Guard モジュール）の一般的なケアや保守用の作業を行う方法について説明します。この章には、次の項があります。

- 設定のエクスポート
- 設定のインポートとアップデート
- Guard モジュールのリロード
- Guard モジュールのリブート
- Guard モジュールのバージョンのアップグレード
- MP 関連のコマンド
- 忘失パスワードの復旧
- 工場出荷時のデフォルト設定へのリセット

設定のエクスポート

Guard モジュールの設定ファイルを FTP サーバまたは SFTP サーバにエクスポートできます。Guard モジュールまたはゾーンの設定ファイル（running-config）をリモート サーバにエクスポートすると、次のことが可能になります。

- Guard モジュールの設定パラメータを別の Guard モジュールに実装する。
- Guard モジュールの設定をバックアップする。

Guard モジュールの設定ファイルをエクスポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy** [**zone** *zone-name*] **running-config ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **running-config sftp** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 12-1 で、**copy running-config ftp** コマンドの引数について説明します。

表 12-1　copy running-config ftp コマンドの引数

パラメータ	説明
zone-name	（オプション）ゾーン名。ゾーンの設定ファイルをエクスポートします。デフォルトでは、Guard モジュールの設定ファイルがエクスポートされます。
running-config	Guard モジュールの設定全体、または指定したゾーンの設定をエクスポートします。
ftp	設定を FTP サーバにエクスポートします。
sftp	設定を SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。

表 12-1　copy running-config ftp コマンドの引数（続き）

パラメータ	説明
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy running-config ftp 10.0.0.191 run-conf.txt <user> <password>
```

設定のインポートとアップデート

Guard モジュールまたはゾーンの設定ファイルを FTP サーバからインポートし、新しく転送されたファイルに応じて Guard モジュールを再設定できます。次の目的で設定をインポートします。

- Guard モジュールの既存の設定ファイルに基づいて Guard モジュールを設定する。
- Guard モジュールの設定を復元する。

ゾーンの設定は、Guard モジュールの設定の一部です。**copy ftp running-config** コマンドを使用して、両方のタイプの設定ファイルを Guard モジュールにコピーし、それに応じて Guard モジュールを再設定します。

（注） 既存の設定が新しい設定で上書きされます。新しい設定を有効にするには、Guard モジュールをリロードする必要があります。

すべてのゾーンを非アクティブにしてからインポート プロセスを開始することをお勧めします。ゾーン設定をインポートする前に、Guard モジュールによってゾーンは非アクティブになります。

デフォルトでは、Guard モジュールは古いバージョンの自己保護設定を無視します。自己保護設定を古い設定で上書きしないでください。古い設定は現在の設定と互換性がない場合があります。

Guard モジュールの設定ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy sftp running-config** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 12-2 で、**copy ftp running-config** コマンドの引数について説明します。

表 12-2　copy ftp running-config コマンドの引数

パラメータ	説明
zone-name	（オプション）ゾーン名。ゾーンの設定ファイルをエクスポートします。デフォルトでは、Guard モジュールの設定ファイルがエクスポートされます。
ftp	設定を FTP サーバからインポートします。
sftp	設定を SFTP サーバからインポートします。
server	サーバの IP アドレス。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリでファイルを検索します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy ftp running-config 10.0.0.191 scannet-conf <user> <password>
```

古いバージョンからエクスポートした設定をインポートすると、Guard モジュールによって次のメッセージが表示されます。

```
WARNING: The configuration file includes a self-protection definition
that is incompatible with the current version and will be ignored.
Continue? [yes|no]
```

次のいずれかのオプションを入力します。

- yes：古い自己保護設定を無視します。Guard モジュールは次のように動作します。
  - 古い自己保護設定を無視し、インポートしない。
  - ゾーン、インターフェイス、サービス設定など、他の設定をすべてインポートする。
- no：古い自己保護設定をインポートできます。Guard モジュールによって次のメッセージが表示されます。

```
You can abort the import process or import the old self-protection
definition as-is.
WARNING: The self-protection definitions are incompatible with the
current version.
Abort? [yes|no]
```

注意　自己保護設定を古い設定で上書きしないでください。古い設定は現在の設定と互換性がない場合があります。

古い自己保護設定をインポートするには、no を入力します。

インポート プロセスを打ち切るには、yes を入力します。

Guard モジュールのリロード

reload コマンドを使用すると、マシンをリブートすることなく Guard モジュールの設定をリロードできます。

次の変更内容を反映するには、Guard モジュールをリロードする必要があります。

- **shutdown** コマンドによる物理インターフェイスの非アクティブ化またはアクティブ化
- 新しいフラッシュの組み込み

Guard モジュールのリブート

デフォルトの動作では、Guard モジュールはすべてのゾーンを非アクティブの動作状態でロードします。そのため、リブート前のゾーンの動作状態に関係なく、Guard モジュールはリブート後にゾーン保護またはラーニング プロセスをイネーブルにしません。

リブート プロセス前にアクティブであったゾーンが Guard モジュールによって自動的にアクティブになるように、デフォルトの動作を変更するには、設定モードで次のコマンドを入力します。

boot reactivate-zones

注意　ゾーンのラーニング フェーズは、リブート後に再起動されます。

Guard モジュールのバージョンのアップグレード

Guard モジュールが動作するためには、次の 2 つのソフトウェア コンポーネントが必要です。

- Supervisor 2 エンジンまたは Supervisor 720 エンジンを使用する Cisco IOS イメージ
- Guard モジュール ソフトウェア

（注） バージョンをアップグレードするには、Supervisor Engine モジュールにログインする必要があります。

Supervisor 2 または Supervisor 720 を使用する IOS ソフトウェア イメージ

1 つ目のソフトウェア コンポーネントは、Catalyst 6500 Supervisor 2 エンジンまたは Supervisor 720 エンジン（スーパーバイザ）を使用する Cisco IOS イメージです。スーパーバイザ モジュール上のイメージは、Guard モジュールおよびそのプロセッサを認識して初期化します。Guard モジュールをサポートする Cisco IOS イメージを使用する必要があります。

Guard モジュール ソフトウェア

Guard モジュール ソフトウェアは、プロセッサ制御複合体に統合された Compact Flash（CF; コンパクト フラッシュ）カードに常駐します。コンパクト フラッシュには、ソフトウェア イメージのパーティションが 2 つあります。それぞれには独自のオペレーティング システム（イメージ）が用意されています。

- メンテナンス　パーティション（MP）：基本モジュールの初期化およびドーター カードの制御の機能のために必要なソフトウェア（cf:1 と呼ばれる）
- アプリケーション パーティション（AP）：Guard モジュール アプリケーションに付属するイメージ（cf:4 と呼ばれる）

コンパクト フラッシュ カード上の Guard モジュール ソフトウェアは、スーパーバイザ コンソールを使用してアップグレードできます。このアップグレード プロセスでは、最新バージョンの AP イメージや MP イメージを Cisco Software Center から FTP サーバまたは TFTP サーバにダウンロードし、コンパクト フラッシュ カードにインストールします。

標準のアップグレード手順には、スーパーバイザから Guard モジュールのコンパクト フラッシュにある AP および MP イメージをアップグレードする作業が含まれます。

Guard モジュールでは、次のアップグレード手順を使用できます。

- AP のアップグレード手順：アプリケーション イメージを使用可能な最新バージョンにアップグレードします。この手順は MP から実行し、モジュールをリセットする必要があります。P.12-11 の「AP のアップグレード手順」を参照してください。
- MP のアップグレード手順：メンテナンス パーティションをアップグレードします。MP イメージは、アップグレードの必要がほとんどありません。この手順は、バージョン リリースに付属のリリース ノートで指示されている場合にのみ使用してください。P.12-14 の「MP のアップグレード手順」を参照してください。
- インライン イメージのアップグレード手順：アプリケーション イメージまたはメンテナンス イメージをアップグレードします。この手順は MP から実行します。P.12-17 の「インライン アップグレード手順」を参照してください。

アップグレード時の注意事項

この項では、AP および MP のバージョンをアップグレードする際のガイドラインを示します。

- AP および MP のバージョンをアップグレードするには、スーパーバイザにログインします。Guard モジュールのフラッシュ（CFE）をアップグレードするには、Guard モジュールにログインします。
- AP イメージと MP イメージの両方をアップグレードする場合は、MP イメージを先にアップグレードする必要があります。
- MP に切り替えるには、**hw-module module** *slot_number* **reset cf:1** コマンドを使用します。MP モードで操作する主な目的は、AP イメージをアップグレードすることです。
- AP に切り替えるには、**hw-module module** *slot_number* **reset cf:4** コマンドを使用します。AP が通常の動作モードです。

- **show module** コマンドを使用すると、実行しているパーティション イメージのソフトウェア バージョンを表示できます。AP イメージを実行している場合、**show module** コマンドを使用すると AP イメージのバージョンが表示されます。AP イメージのバージョンの形式は、*4.0(0.12)* のようになります。MP イメージを実行している場合は、MP イメージのバージョンが表示されます。MP イメージのバージョンの形式は、*4.0(0.0)m* のようになります。
- MP イメージ ファイル名の形式は、*MPUpgrade-4.0.0.0.bin* です。
- AP イメージ ファイル名の形式は、*AGM-APUpgrade-4.0.0.12.bin* です。
- MP は Guard モジュールと同じネットワーク設定を使用します。Guard モジュールのイメージをアップグレードする前に、ネットワークの設定を行う必要があります。詳細については、第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」および第 3 章「Guard モジュールの初期化」を参照してください。
- AP をアップグレードするときに、Guard モジュールは自己保護設定を新しい設定で更新します。自己保護設定を古い設定で上書きしないでください。古い設定は現在の設定と互換性がない場合があります。

（注） スーパーバイザで **logging console** コマンドをグローバルに設定して、アップグレード手順の詳細な出力を表示することを強くお勧めします。コンソールではなく Telnet セッションから接続している場合、コンソール メッセージを表示するには **terminal monitor** コマンドを使用します。

AP のアップグレード手順

アプリケーション イメージをアップグレードするには、次の手順を実行します。

ステップ 1　アップグレード プロセスを開始する前に、**copy running-config** コマンドを使用して Guard モジュールの設定をバックアップします。詳細については、P.12-2 の「設定のエクスポート」を参照してください。

ステップ 2　アプリケーション イメージを使用可能な最新バージョンにアップグレードするには、まず、次の場所にある Cisco.com の Software Center でイメージを見つけます。

http://www.cisco.com/public/sw-center/

FTP または TFTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

ステップ 3　Guard モジュールをリセットし、MP イメージをロードします（この処理には約 3 分かかります）。すでに MP イメージを実行している場合は、このステップを省略します。

スーパーバイザで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 4　MP がブートされ、Guard モジュールのステータスが OK であることを確認します。次のコマンドを入力します。

```
show module slot_number
```

ステップ 5　AP イメージをコンパクト フラッシュにインストールします。この処理には数分かかる場合があります。次のコマンドを入力します。

copy tftp://*path***/***filename* **pclc#***slot_number***-fs:**

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に *ftp://user@host/absolute-path/filename* という構文を使用します。パスワードを要求されたら入力します。

また、FTP サーバから目的のバージョンをダウンロードすることもできます。

アプリケーション イメージのダウンロードの所要時間は、接続の速度によって異なりますが、最大で約 30 分です。

注意　Guard モジュールのコンソールに次のメッセージが表示されるまでは、モジュールをリセットしないでください。

```
You can now reset the module
```

このメッセージが表示される前にモジュールをリセットすると、アップグレードが失敗します。

ステップ 6　Guard モジュールを AP にリセットします。次のコマンドを入力します。

hw-module module *slot_number* **reset cf:4**

ステップ 7　コピーした AP イメージが **show module** コマンドの出力に表示されることを確認します。次のコマンドを入力します。

show module *slot_number*

（注） 新しいバージョンで Common Firmware Environment（CFE）のアップデートが必要になることがあります。詳細については、各バージョン リリースに付属のリリース ノートを参照してください。CFE が適合していない場合、AP イメージのアップグレードの後でユーザが最初に Guard モジュールへのセッションを確立すると、Guard モジュールは次のメッセージを表示します。

```
Bad CFE version (X). This version requires version Y
```

詳細については、P.12-21 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

次の例は、AP イメージをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified. <<< このメッセージは、情報提供用です。

Proceed with reload of module? [confirm]

% reset issued for module 8
Sup# copy tftp:images/ap/AGM-APUpgrade-4.0.0.x.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/AGM-APUpgrade-4.0.0.x.bin]?
Destination filename [AGM-APUpgrade-4.0.0.x.bin]?
.
.
.
19:50:06: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has started>
19:50:06: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till upgrade completes!!>

......<<< Wait

19:59:58: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has succeeded>
19:59:58: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>

Sup# hw-module module 8 reset cf:4 <<<<< Guard モジュールを AP へリセット
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
...
%OIR-SP-6-INSCARD:Card inserted in slot 8, interfaces are now online
```

MP のアップグレード手順

MP イメージは、アップグレードの必要がほとんどありません。MP イメージをアップデートするようバージョン リリースに付属のリリース ノートで指示されている場合、次の手順を実行します。

ステップ 1　イメージを使用可能な最新バージョンにアップグレードするには、まず、次の場所にある Cisco.com の Software Center でイメージを見つけます。

http://www.cisco.com/public/sw-center/

FTP または TFTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

ステップ 2　Guard モジュールをリセットし、MP イメージをロードします（この処理には約 3 分かかります）。すでに MP イメージを実行している場合は、このステップを省略します。

スーパーバイザで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 3　MP がブートされ、Guard モジュールのステータスが OK であることを確認します。次のコマンドを入力します。

```
show module slot_number
```

ステップ 4　MP イメージをコンパクト フラッシュにコピーします。Guard モジュールが MP または AP にリセットされているときに、MP イメージをコピーできます。

スーパーバイザで次のコマンドを入力します。

```
copy tftp://path/filename pclc#slot_number-fs:
```

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。

FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に *ftp://user@host/absolute-path/filename* という構文を使用します。パスワードを要求されたら入力します。

アプリケーション イメージのダウンロードの所要時間は、接続の速度によって異なりますが、最大で約 30 分です。

注意　Guard モジュールのコンソールに次のメッセージが表示されるまでは、モジュールをリセットしないでください。

```
You can now reset the module
```

このメッセージが表示される前にモジュールをリセットすると、アップグレードが失敗します。

また、FTP サーバから目的のバージョンをダウンロードすることもできます。

MP コマンドの詳細については、P.12-23 の「MP 関連のコマンド」を参照してください。

ステップ 5　コピーした MP イメージが **show module** コマンドの出力に表示されることを確認します。

show module *slot_number*

ステップ 6　Guard モジュールを AP にリセットします。次のコマンドを入力します。

hw-module module *slot_number* **reset cf:4**

次の例は、MP イメージをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified. <<< このメッセージは、情報提供用です。

Proceed with reload of module? [confirm]

% reset issued for module 8
Sup# copy tftp:images/mp/MPUpgrade-4.0.0.0.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/MPUpgrade-4.0.0.0.bin]?
Destination filename [MPUpgrade-4.0.0.0.bin]?
.
.
.
3d19h:%SVCLC-SP-5-STRRECVD:mod 8:<Upgrade of MP was successful.>
3d19h:%SVCLC-SP-5-STRRECVD:mod 8:<You can now reset the module>
Sup# show module 8
.
Guard モジュールが MP (cf:1) へリセットされたことで、次のような MP イメージ名が
表示されます。
.
Mod  MAC addresses                       Hw    Fw      Sw          Status
---  ----------------------------------- ------- ----------- -------
8    000f.348d.d7f0 to 000f.348d.d7f70.301 7.2(1)  4.0(0.0)m   Other
...
Sup# hw-module module 8 reset cf:4 <<< Guard モジュールを AP へリセット
(通常動作)
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
...
%OIR-SP-6-INSCARD:Card inserted in slot 8, interfaces are now online
```

インライン アップグレード手順

インライン イメージのアップグレード手順は、AP イメージおよび MP イメージをアップグレードする代替の方法です。

イメージをアップグレードするには、次の手順を実行します。

ステップ 1　アップグレード プロセスを開始する前に、**copy running-config** コマンドを使用して Guard モジュールの設定をバックアップします。詳細については、P.12-2 の「設定のエクスポート」を参照してください。

ステップ 2　イメージを使用可能な最新バージョンにアップグレードするには、まず、次の場所にある Cisco.com の Software Center でイメージを見つけます。

http://www.cisco.com/public/sw-center/

FTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

MP コマンドの詳細については、P.12-21 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

ステップ 3　コンソール ポートまたは Telnet セッションを介してスーパーバイザにログインします。

ステップ 4　Guard モジュールをメンテナンス イメージで実行している場合は、ステップ 6 に進みます。Guard モジュールをメンテナンス イメージで実行していない場合は、スーパーバイザで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 5　Guard モジュールがオンラインに戻ったら、Guard モジュールとのコンソール セッションを確立し、ルート アカウントにログインします。アカウントのデフォルト パスワードは *cisco* です。

ステップ 6　イメージをアップグレードします。次のコマンドを入力します。

```
upgrade ftp://path/filename
```

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。

FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に *ftp://user@host/absolute-path/filename* という構文を使用します。パスワードを要求されたら入力します。

AP イメージをアップグレードするには、AP イメージのファイル名を入力します。MP イメージをアップグレードするには、MP イメージのファイル名を入力します。詳細については、P.12-9 の「アップグレード時の注意事項」を参照してください。

注意　Guard モジュールのコンソールに次のメッセージが表示されるまでは、モジュールをリセットしないでください。

```
Application image upgrade complete.You can boot the image now.
```

このメッセージが表示される前にモジュールをリセットすると、アップグレードが失敗します。

ステップ 7　アップグレードが完了したら、Guard モジュールからログアウトします。**exit** コマンドを使用します。

ステップ 8　Guard モジュールを AP イメージにリセットします。次のコマンドを入力します。

```
hw-module module slot_number reset cf:4
```

（注） 新しいバージョンで Common Firmware Environment（CFE）のアップデートが必要になることがあります。詳細については、各バージョン リリースに付属のリリース ノートを参照してください。CFE が適合していない場合、AP イメージのアップグレードの後でユーザが最初に Guard モジュールへのセッションを確立すると、Guard モジュールは次のメッセージを表示します。

```
Bad CFE version (X). This version requires version Y
```

詳細については、P.12-21 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

ステップ 9　Guard　モジュールがリブートしたら、ソフトウェア　バージョンを確認します。**show version** コマンドを使用します。

次の例は、Guard モジュールのアプリケーション ソフトウェアをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
.
.
.
Proceed with reload of module? [confirm]
% reset issued for module 9
.
.
.
Sup# session slot 8 proc 1
.
.
.
login:root
Password:
.
.
.
root@localhost.cisco.com# upgrade
ftp://psdlab-pc1/pub/images/ap/AGM-APUpgrade-4.0.0.x.bin


Downloading the image. This may take several minutes...
.
.
.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:



Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.
.
.
.
Application image upgrade complete. You can boot the image now.
root@hostname.cisco.com# exit
logout
                                                                [  OK  ]
[Connection to 127.0.0.91 closed by foreign host]
Sup# hw-module module 8 reset cf:4
```

新しいフラッシュ バージョンの焼き付け

現在の Common Firmware Environment（CFE）とソフトウェア バージョンが適合していない場合にだけ、新しいフラッシュ バージョンを焼き付けることができます。不適合は、Guard ソフトウェアをアップデートするときに発生する場合があります。

CFE との不適合が検出された場合、ソフトウェア バージョンのアップグレード後に Guard モジュールとの最初のセッションを確立するときに、Guard モジュールは次のメッセージを表示します（X は古いフラッシュ バージョンを示し、Y は新しいフラッシュ バージョンを示します）。

```
Bad CFE version (X). This version requires version Y
```

注意　新しいフラッシュ バージョンを焼き付けている間は、Guard モジュールに安定して電源が供給されるようにし、かつ Guard モジュールを動作させないようにする必要があります。こうした制約事項に従わないと、アップグレードが失敗して Guard モジュールにアクセスできなくなる場合があります。

新しいフラッシュ バージョンを焼き付けるには、次の手順を実行します。

ステップ 1　設定モードで次のコマンドを入力します。

```
flash-burn
```

CFE と Guard モジュールのソフトウェア バージョンが適合している場合に新しいフラッシュを焼き付けようとすると、操作が失敗します。

ステップ 2　Guard モジュールをリロードします。次のコマンドを入力します。

```
reload
```

新しいフラッシュ バージョンを焼き付けた後、reload コマンドを発行する必要があります。Guard は、reload コマンドを実行した後でないと完全に機能しません。

次の例を参考にしてください。

```
user@GUARD-conf# flash-burn
Please note: DON'T PRESS ANY KEY WHILE IN THE PROCESS!
. . .
Burned firmware successfully
SYSTEM IS NOT FULLY OPERATIONAL. Type 'reload' to restart the system
```

MP 関連のコマンド

管理者は Guard モジュールを MP からブートすることができます。Guard モジュールを管理および診断するため、インターフェイスのセットを MP で使用できます。MP の主要な特徴の 1 つは、新しい AP イメージをインストールする機能を提供することです。

MP からブートするには、**hw_module module reset** コマンドを使用します。次に、**session slot** コマンドを使用して MP にログインします。

表 12-3 は MP コマンドを要約したものです。

表 12-3　MP 関連のコマンド

コマンド	説明
clear ap password	Guard モジュールに定義されたすべてのパスワードを消去します。
clear ap config	Guard モジュールをデフォルト設定に戻します。このコマンドは Guard モジュールの設定、ログ、およびレポートをすべて削除します。
ip address [*ip address*] [*subnet*]	Guard モジュールが外部ネットワークへのアクセスに使用する IP アドレスを設定します。
ip gateway [*default-gateway*]	ネットワークのデフォルト ゲートウェイを指定します。
passwd	現行ユーザのパスワードを変更します。
passwd-guest	ゲスト アカウントのパスワードを変更します。
ping {*host-name* | *ip address*}	ネットワーク上の特定のホストに ping を実行し、ネットワーク パラメータが正しく設定されていることを確認します。
show images	アプリケーション パーティションに格納されているイメージを表示します。
show ip	Guard モジュールのネットワーク パラメータを表示します。
upgrade *ftp-url*	イメージをアップグレードします。*ftp-url* は、イメージおよびイメージへのパスを含む FTP サーバを指定する URL です。パスの形式は *ftp://user:password@server-name/path* です。 FTP サーバの名前または IP アドレスを指定できます。

忘失パスワードの復旧

この項では、忘失したパスワードを復旧する方法について説明します。

忘失したパスワードを復旧するには、次の手順を実行します。

ステップ 1　Guard モジュールを MP にリセットします。スーパーバイザで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 2　Guard モジュールがオンラインに戻ったら、Guard モジュールとのセッションを確立し、ルート アカウントにログインします。

ステップ 3　Guard モジュールに設定されたすべてのパスワードを消去します。次のコマンドを入力します。

```
clear ap password
```

ステップ 4　Guard モジュールを AP にリセットします。次のコマンドを入力します。

```
hw-module module slot_number reset cf:4
```

ステップ 5　Guard モジュールに設定されたユーザに、新しいパスワードを設定します。P.4-10 の「パスワードの変更」を参照してください。Guard モジュールのユーザのリストを表示するには、**show running-config** コマンドを使用します。

ヒント　**show running-config** コマンド出力の表示を Guard モジュールのユーザのリストだけが含まれるように絞り込むには、**show running-config | include username** コマンドを使用します。

工場出荷時のデフォルト設定へのリセット

状況に応じて、Guard モジュールの設定を工場出荷時のデフォルト設定に復元することができます。これは、Guard モジュールに存在する不要な設定を取り除く場合に役立ちます。Guard モジュールを設定した結果、その設定内容が非常に複雑になった場合や、あるいは Guard モジュールをあるネットワークから別のネットワークに移動する場合などが考えられます。Guard モジュールを工場出荷時のデフォルト設定にリセットし、新しい Guard モジュールとして設定することができます。

工場出荷時のデフォルト設定にリセットする前に、**copy running-config** コマンドを使用して Guard モジュールの設定をバックアップしておくことをお勧めします。P.12-2 の「設定のエクスポート」を参照してください。

管理インターフェイスの設定（eth1）は、Guard モジュールをリロードするまで使用できます。

Guard モジュールを工場出荷時のデフォルト設定にリセットするには、設定モードで次のコマンドを入力します。

clear config all

設定した変更内容は、リセットをした後に有効になります。

注意　コンソールから接続していないときに、Guard モジュールの設定を工場出荷時のデフォルト設定にリセットして Guard モジュールをリロードすると、Guard モジュールへの接続は失われます。

次の例を参考にしてください。

```
user@GUARD-conf# clear config all
```

CHAPTER 13

Guard モジュールによる軽減の分析

この章では、Cisco Anomaly Guard Module（Guard モジュール）による軽減およびゾーンのトラフィックを分析する方法、および設定の問題を識別する方法のガイドラインを示します。また、攻撃のタイプを識別する方法について簡単に説明します。この章は、次の項で構成されています。

- ゾーンのトラフィック パターンの分析
- 攻撃の軽減の確認

ゾーンのトラフィック パターンの分析

ゾーンの通常のトラフィック レートを前もって知っておくと、ゾーンへの異常なトラフィックを簡単に認識できます。

オンデマンド ゾーンである場合、または最後にラーニング プロセスを実行してからゾーンのトラフィック特性が変わった場合は、現在の攻撃が終了してから Guard モジュールにゾーンのトラフィック パターンをラーニングさせることを強くお勧めします。

ゾーンの現在のトラフィック レートを表示するには、**show rates** コマンドを使用します。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。

受信トラフィック レートを表示する場合は、次の点に注意してください。

- 受信レートがゼロの場合は、宛先変更の問題が発生していることを示します。詳細については、P.13-3 の「宛先変更の問題」を参照してください。
- 受信レートが正当なトラフィックのレートよりも高い場合は、Guard モジュールによる軽減が機能していることを示します。
  - 正当なトラフィックのレートが、認識しているゾーン トラフィックに比べて高すぎる場合は、P.13-3 の「フロー特性に基づくゾーンへのフローのブロッキング」を参照してください。
  - 正当なトラフィックのレートが、認識しているゾーン トラフィックに比べて低すぎる場合は、P.13-5 の「トラフィック ブロッキング基準の確認」を参照してください。

宛先変更の問題

Guard モジュールがパケットをまったく受信しない場合は、宛先変更の問題が発生している可能性があります。宛先変更の問題が発生していると、Guard モジュールは、ゾーンに送信されたトラフィックを受信しません。

宛先変更が正しく設定されていることを確認してください。詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

次のガイドラインを使用します。

- 宛先変更のルートが正しく設定されていることを確認する。詳細については、P.5-9 の「宛先変更ルートの表示」を参照してください。
- ハイジャック VLAN がブロックされないことを確認する。スーパーバイザからハイジャック インターフェイスに ping を実行してください。

フロー特性に基づくゾーンへのフローのブロッキング

正当なトラフィックのレートが、認識しているゾーン トラフィック特性から判断して高すぎると思われる場合は、Guard モジュールが一部の攻撃トラフィックをブロックしていない可能性があります。この現象は、ラーニング プロセスが実行されなかったオンデマンド ゾーンで発生することがあります。このような場合は、そのゾーンで、オンデマンド ポリシーしきい値が大きすぎる可能性があります。

次の作業を行うことをお勧めします。

- 送信元 IP アドレスに応じてトラフィックを測定するポリシーのしきい値を小さくする。
- 正当なトラフィック レートを確認する。それでも正当なトラフィックのレートが高すぎると思われる場合は、高度かつ大規模なゾンビ攻撃またはクライアント攻撃が発生している可能性があります。このような攻撃は、レートや接続数が通常のフローと変わらない多くのフローで構成されています。このような異常トラフィック フローをブロックするには、フレックスコンテンツ フィルタを設定します。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」を参照してください。

ポリシーのしきい値を小さくするには、次の手順を実行します。

ステップ 1　ポリシーの現在のしきい値を表示します。関連するゾーン設定モードで次のコマンドを入力します。

```
show policies
```

ポリシーの詳細については、P.8-34 の「ポリシーの表示」を参照してください。

ステップ 2　ゾーンのグローバル トラフィックを調べます。次のコマンドを入力します。

```
show policies */*/*/*/global statistics
```

Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、保護ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。サービス タイプおよびトラフィック量がゾーンのトラフィックを表すかどうかを判断します。ポリシーの統計情報の詳細については、P.8-36 の「ポリシーの統計情報の表示」を参照してください。

ステップ 3　送信元 IP アドレスによって示される、個々のユーザのトラフィックを調べます。どのポリシーのしきい値が大きく、小さくする必要があるかを判断します。次のコマンドを入力します。

```
show policies */*/*/*/src_ip statistics
```

Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、保護ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。ポリシーの統計情報の詳細については、P.8-36 の「ポリシーの統計情報の表示」を参照してください。

ステップ 4　トラフィック量がゾーンのトラフィックを表さない場合は、送信元 IP アドレスのポリシーのしきい値を小さくします。次のコマンドを入力します。

```
policy */*/*/*/src_ip thresh-mult threshold-multiply-factor
```

threshold-multiply-factor 引数は、ポリシーのしきい値に掛ける値です。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。たとえば、しきい値を半分にするには、0.5 と入力します。詳細については、P.8-27 の「係数によるしきい値の乗算」を参照してください。

トラフィック ブロッキング基準の確認

正当なトラフィックのレートが低すぎると思われる場合は、Guard モジュールが正当なクライアントからゾーンへのアクセスをブロックしている可能性があります。この現象は、ラーニング プロセスがかなり前に実行されたために、現在ではポリシーのしきい値がゾーンのトラフィック パターンに合わなくなってしまった場合に発生することがあります。その結果、ポリシーのしきい値が適切に調整されておらず、小さくなっています。

Guard モジュールのブロッキング基準を確認および変更するには、次の手順を実行します。

ステップ 1　Guard　モジュールが正当なクライアントからゾーンへのアクセスをブロックしているのではないかと思われる場合は、Guard モジュールの動的フィルタがこのようなクライアントからのアクセスをブロックしていないかどうか確認します。次のコマンドを入力します。

```
show dynamic-filters [details]
```

動的フィルタの詳細については、P.7-34 の「動的フィルタの表示」を参照してください。動的フィルタでは、動的フィルタが生成される原因となったポリシーの詳細が提供されます。

ステップ 2　このようなポリシーの統計情報を表示します。たとえば、送信元 IP アドレスによって示される、個々のユーザのトラフィックを調べます。どのポリシーのしきい値が小さく、大きくする必要があるかを判断します。次のコマンドを入力します。

```
show policies */*/*/*/src_ip statistics
```

Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、保護ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。ポリシーの統計情報の詳細については、P.8-36 の「ポリシーの統計情報の表示」を参照してください。

ステップ 3　トラフィック量がゾーンのトラフィックを表さない場合は、しきい値を大きくします。関連するゾーン設定モードで次のコマンドを入力します。

policy */*/*/*/src_ip thresh-mult *threshold-multiply-factor*

threshold-multiply-factor 引数は、ポリシーのしきい値に掛ける値です。ポリシーのしきい値を大きくするには、1 より大きい数値を入力します。たとえば、しきい値を 2 倍にするには、2 と入力します。詳細については、P.8-27 の「係数によるしきい値の乗算」を参照してください。

ステップ 4　動的フィルタのリストを表示します（ステップ 1 を参照してください）。動的フィルタのリストに *drop* アクションを持つ、正当なクライアントの IP アドレスに対する動的フィルタが含まれている場合、その動的フィルタを削除します。次のコマンドを入力します。

no dynamic-filter *filter-id*

動的フィルタの詳細については、P.7-31 の「動的フィルタの設定」を参照してください。

ステップ 5　Guard　モジュールが引き続き特定のポリシーから　drop　アクションを持つ動的フィルタを生成する場合は、そのポリシーを非アクティブにします。次のコマンドを入力します。

```
state inactive
```

詳細については、P.8-22 の「ポリシーの状態の変更」を参照してください。

ヒント　同じポリシー ブランチに属する複数のポリシーが、drop アクションを持つ動的フィルタを生成する場合は、そのポリシー ブランチを非アクティブにすることができます。

ステップ 6　ゾーンが正しく機能するために不可欠であると分かっているクライアント IP アドレスが Guard モジュールの保護メカニズムをバイパスするように設定します。このようなクライアントの IP アドレスをバイパス フィルタに追加します。Guard モジュールは、このようなトラフィック フローをゾーンに直接転送します。次のコマンドを入力します。

bypass-filter *row-num ip-address protocol dest-port fragments-flag*

詳細については、P.7-21 の「バイパス フィルタの設定」を参照してください。

攻撃の軽減の確認

ゾーンに対する攻撃を識別した場合は、Guard モジュールがその攻撃を軽減していることを確認できます。これは、ゾーンのトラフィック パターンを熟知していない場合、またはゾーンがオンデマンド保護中で、Guard モジュールがゾーンのトラフィック パターンをラーニングしなかった場合に特に重要です。

次の作業を行うことができます。

- ゾーンの現在の攻撃レポートを表示する。詳細については、P.13-8 の「ゾーンの現在の攻撃レポートの表示」を参照してください。
- Guard モジュールのフィルタ、カウンタ、および統計情報を表示する。これを行うには、Guard モジュールの動作およびメカニズムを熟知している必要があります。

ゾーンの現在の攻撃レポートの表示

進行中の攻撃のレポートを表示して、攻撃の特性、および Guard モジュールが攻撃を軽減するために講じた対策を知ることができます。

進行中の攻撃の攻撃レポートを表示するには、**show reports current** コマンドを使用します。詳細については、P.10-14 の「攻撃レポートの表示」を参照してください。

このレポートには、攻撃に関する詳細が記載されます。攻撃の開始日時、ゾーンのトラフィック フローの一般的な分析、ドロップされたパケットおよび返送されたパケットの分析、Guard モジュールがゾーンのトラフィックで検出したトラフィック異常の詳細、ゾーンを保護する（攻撃を軽減する）ために Guard モジュールが実行した処置などの情報が提供されます。詳細については、P.10-2 の「レポートのレイアウトについて」を参照してください。

このレポートには、攻撃の分類に関する詳細が記載されます。DDoS 攻撃は、次のような 2 つの主なクラスに分類されます。

- **帯域幅の枯渇**：正当なトラフィックがゾーンに到達できないようにする不要なトラフィックをゾーンに多量に注入するための攻撃。このような攻撃には、スプーフィングを利用した攻撃や不正な形式のパケットなどがあります。
- **リソースの枯渇**：ゾーンのリソースを使い果たしてしまうための攻撃。

軽減された攻撃のタイプの詳細については、P.10-6 の「Mitigated Attacks」を参照してください。

Guard モジュールの高度な統計情報の表示

Guard モジュールのフィルタ、カウンタ、および診断情報を表示して、攻撃の特性、および Guard モジュールが攻撃を軽減するために講じた対策を詳細に知ることができます。このような手順を実行するには、Guard モジュールの動作およびメカニズムを熟知している必要があります。

次の情報を表示できます。

- **動的フィルタ**：このフィルタでは、Guard モジュールが攻撃を処理している方法の詳細が提供されます。動的フィルタを表示するには、**show dynamic-filters** コマンドを使用します。詳細については、P.7-34 の「動的フィルタの表示」を参照してください。
- **ユーザ フィルタ**：このフィルタでは、DDoS 攻撃ではないかと思われるトラフィック フローを処理する方法が定義されます。ゾーンの設定には、デフォルトのユーザ フィルタのセットが含まれます。ユーザ フィルタを追加または削除できます。ユーザ フィルタを表示するには、**show** コマンドまたは **show running-config** コマンドを使用します。Guard モジュールは、各ユーザ フィルタで測定された現在のトラフィック レートを表示します。詳細については、P.7-28 の「ユーザ フィルタの表示」を参照してください。
- **ドロップされたパケットに関する統計情報**：この統計情報では、進行中の攻撃のドロップされたパケットの分布を示すリストが提供されます。ドロップされたパケットに関する統計情報を表示するには、**show drop-statistics** コマンドを使用します。詳細については、P.13-10 の「ドロップされたトラフィックの統計情報の表示」を参照してください。
- **ゾーンのレート履歴**：このリストには、Guard モジュールが過去 24 時間に各カウンタで測定したレートが表示されるため、攻撃の展開に関する詳細が分かります。ゾーンのレート履歴を表示するには、**show rates history** コマンドを使用します。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。
- **ゾーンのカウンタ**：このリストには、Guard モジュールが各カウンタで測定したパケット数が表示されるため、攻撃開始後に Guard モジュールがゾーンのトラフィックを処理した方法を分析できます。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。

ドロップされたトラフィックの統計情報の表示

進行中の攻撃のドロップされたパケットの分布を表示できます。Guard モジュールは、保護メカニズムによってドロップされたパケットをレート、パケット、およびビット単位で表示します。

次のコマンドを入力します。

show drop-statistics

表 13-1 で、ドロップ統計情報について説明します。

表 13-1　ドロップ統計情報

タイプ	説明
Total dropped	ドロップされたトラフィックの合計量。
Dynamic filters	動的フィルタによってドロップされたトラフィックの量。
User filters	ユーザ フィルタによってドロップされたトラフィックの量。
Flex-Content filter	フレックスコンテンツ フィルタによってドロップされたトラフィックの量。
Rate limit	ゾーンのレート リミット保護モジュールによってドロップされたパケットを示します。これらのパケットは、ユーザ フィルタのレート リミット パラメータ、およびゾーンの **rate-limit** コマンドによって定義されます。
Incoming TCP unauthenticated basic	基本的な TCP スプーフィング防止メカニズムによって認証されなかったためにドロップされたトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Incoming TCP unauthenticated-strong	強力な TCP スプーフィング防止メカニズムによって認証されなかったためにドロップされたトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。

表 13-1　ドロップ統計情報（続き）

タイプ	説明
Outgoing TCP unauthenticated	TCP スプーフィング防止メカニズムによって認証されなかったためにドロップされた、ゾーンで開始された接続のトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
UDP unauthenticated-basic	基本的なスプーフィング防止メカニズムによって認証されなかったためにドロップされた UDP トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
UDP unauthenticated-strong	強力なスプーフィング防止メカニズムによって認証されなかったためにドロップされた UDP トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
Other protocols unauthenticated	Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、TCP および UDP 以外のトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
TCP fragments unauthenticated	Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、断片化された TCP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
UDP fragments unauthenticated	Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、断片化された UDP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。

表 13-1　ドロップ統計情報（続き）

タイプ	説明
Other protocols fragments unauthenticated	Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、TCP および UDP 以外の断片化されたパケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
DNS malformed replies	Guard の保護メカニズムによってドロップされた不正な形式の DNS 応答。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
DNS spoofed replies	Guard のスプーフィング防止メカニズムによってドロップされた、ゾーンで開始された接続に応答する着信 DNS パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。
DNS short queries	Guard の保護メカニズムによってドロップされた短い（不正な形式の）DNS クエリー。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
NON DNS packets to DNS port	Guard の保護メカニズムによってドロップされた、DNS ポート宛ての非 DNS トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
Bad packets to proxy addresses	Guard の保護メカニズムによってドロップされた、Guard モジュールのプロキシ IP アドレス宛ての不正形式トラフィック。
TCP anti-spoofing mechanisms related pkts	Guard モジュールの TCP スプーフィング防止メカニズムの副次的な動作が原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。

表 13-1　ドロップ統計情報（続き）

タイプ	説明
DNS anti-spoofing mechanisms related pkts	Guard モジュールの DNS スプーフィング防止メカニズムの副次的な動作が原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
Anti-spoofing internal errors	Guard モジュールのスプーフィング防止メカニズムのエラーのためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Packets テーブルでカウントされます。
Land attack	送信元 IP アドレスと宛先 IP アドレスが同じであるためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。
Malformed packets	ヘッダーの形式が不正である（ヘッダーのポート、プロトコル、または IP のフィールドがゼロ（0）になっている）ことが原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show drop-statistics
```

INDEX

A

AAA
- アカウンティング 4-17
- 設定 4-5
- 認可 4-14
- 認証 4-7

aaa accounting コマンド 4-17
aaa authentication コマンド 4-7
aaa authorization コマンド 4-14
action コマンド 8-31
add-service コマンド 8-16
Admin 特権レベル 3-2
always-accept 8-33
always-ignore 8-33
anti-spoofing ドロップ統計情報 13-13
AP
- アップグレード 12-11
- アップグレード、インライン 12-17
- ～からのブート 2-12
- 設定の消去 12-23
- パスワードの消去 12-23, 12-24

arp コマンド 11-37
auth パケット タイプ 8-19

B

bad packets to proxy ドロップ統計情報 13-12
basic
- ユーザ フィルタのアクション 7-25

block-unauthenticated ポリシー アクション 8-31
boot コマンド 2-12

C

CFE 12-13, 12-19, 12-21
clear ap config コマンド 12-23
clear ap password コマンド 12-23, 12-24
clear log コマンド 11-12
CLI
- エラー メッセージ 3-5
- コマンドのショートカット 3-7
- コマンドの発行 3-3
- 使用 3-2
- タブ補完 3-6
- プロンプトの変更 4-35
- ヘルプの取得 3-6

Config 特権レベル 3-2
copy コマンド
- ftp running-config 12-4
- packet-dump 11-23
- running-config 12-2

ゾーンのログ　11-11
レポート　10-20
ログ　11-8, 11-11
copy-from-this　6-7
copy-policies コマンド　8-44
cpu 使用率　11-36

D

date コマンド　4-30
DDoS
概要　1-2
攻撃の分類　13-8
deactivate コマンド　6-21, 6-38
default-gateway コマンド　3-14
description コマンド　6-11
diff コマンド　8-41, 8-42
disable コマンド　8-12
Distributed Denial of Service
「DDoS」を参照
DNS
TCP ポリシー テンプレート　8-5
検出された異常　10-5
ドロップ統計情報　13-12, 13-13
drop
動的フィルタのアクション　7-32
ポリシー アクション　8-31
ユーザ フィルタのアクション　7-25
drop-statistics コマンド　13-10
dst トラフィック特性　8-20
Dynamic 特権レベル　3-2

E

enable
password コマンド　4-13
コマンド　4-13, 8-12
event monitor コマンド　11-8
export packet-dump コマンド　11-22
export reports コマンド　10-19
export コマンド　11-10
packet-dump　11-22

F

facility　11-9
filter-termination コマンド　7-39
first-hit　4-21
fixed-threshold　8-25
flash-burn コマンド　12-21
fragments
ポリシー テンプレート　8-5

G

global トラフィック特性　8-20
Guard
自己保護　11-49
複数の設定　2-14

H

hostname
コマンド　4-35
変更　4-35

HTTP
検出された異常 10-5
ポリシー テンプレート 8-5
hw-module コマンド 2-11, 12-11, 12-12, 12-14, 12-17, 12-24

I

in パケット タイプ 8-19
incoming TCP ドロップ統計情報 13-10
interactive-status コマンド 8-32
ip address コマンド
インターフェイス 3-9 - 3-12
ゾーン 6-9, 6-45
ip route コマンド 3-15
IP アドレス
変更、ゾーン 6-10
IP スキャン
検出された異常 10-5
ポリシー テンプレート 8-6

K

key コマンド
add 4-29, 4-31
generate 4-33
remove 4-32

L

land attack ドロップ統計情報 13-13
learning
policy-construction コマンド 6-17
threshold-tuning コマンド 6-20, 6-21
コマンド 6-19, 6-22
learning accept コマンド 6-18, 6-21
learning-params
periodic-action コマンド 6-18, 6-22, 6-25
threshold-multiplier コマンド 8-26
threshold-selection コマンド 6-21, 6-26
threshold-tuned コマンド 6-10, 6-27
learning-params fixed-threshold コマンド 8-25
LINK テンプレート 6-17
logging コマンド 11-9

M

malformed packets ドロップ統計情報 13-13
max-services コマンド 8-10
MIB、サポートされている 4-2
min-threshold コマンド 8-11
MP
アップグレード 12-14
アップグレード、インライン 12-17
～からのブート 2-12
mtu コマンド 3-9, 3-11

N

netstat コマンド 11-40
no learning コマンド 6-19, 6-22
non DNS ドロップ統計情報 13-12
notify ポリシー アクション 8-31
ns ポリシー テンプレート 8-8
num_sources パケット タイプ 8-19

O

other protocols ドロップ統計情報 13-11
other_protocols
ポリシー テンプレート 8-6
outgoing TCP ドロップ統計情報 13-11
out_pkts パケット タイプ 8-19

P

packet-dump 11-14
auto-capture コマンド 11-18
エクスポート 11-22, 11-23
シグニチャ 11-29
自動
アクティブ化 11-16
非アクティブ化 11-18
packet-dump コマンド 11-19
permit
コマンド 3-18, 3-20, 4-3
ユーザ フィルタのアクション 7-25
ping コマンド 11-45
pkts パケット タイプ 8-19
policy set-timeout コマンド 8-30
policy-template add-service コマンド 8-16
policy-template remove service コマンド 8-16
power enable コマンド 2-12
protect learning コマンド 6-20
protect コマンド 6-38
protection-end-timer コマンド 6-43
protocol トラフィック特性 8-20
proxy
コマンド 3-17
proxy-threshold コマンド 8-29

R

Rate Limiter
ドロップされた 13-10
rate-limit コマンド 6-10
rates
履歴 11-4
reactivate-zones 12-7
redirect/zombie
動的フィルタのアクション 7-32
ポリシー アクション 8-31
reload コマンド 12-7
remove service コマンド 8-16
reqs パケット タイプ 8-19
reset コマンド 2-11
running-config
copy 12-2
copy ftp 12-4
show 11-2

S

self-protection コマンド 11-49
service
snmp-trap 4-36
wbm 3-18
コマンド 3-18, 4-3
set-action 8-31
show public-key コマンド 4-33

show コマンド
counters 11-4
cpu 11-36
diagnostic-info 11-34
drop-statistics 13-10
dynamic-filters 7-34, 13-5
host-keys 4-28
log export-ip 11-10
memory 11-35
packet-dump signatures 11-29
rates 11-4, 13-2
recommendations pending-filters 9-8
running-config 11-2
show 11-3
templates 6-7
公開鍵 4-33
推奨事項 9-5, 9-6
ゾーンのポリシー 8-34
動的フィルタのソート 7-34
ポリシー 8-34, 13-4, 13-6
ポリシーの統計情報 6-23, 8-36
モジュール 2-3, 12-11, 12-14, 12-15
レポート 13-8
レポートの詳細 10-14
ロギング 11-10
ログ 11-11
Show 特権レベル 3-2
shutdown コマンド 3-10
snapshot コマンド 8-38
SNMP、アクセス 4-2
snmp コマンド
community 4-38
trap-dest 4-36
SNMP、トラップ ジェネレータの設定 4-36
speed コマンド 3-10
src トラフィック特性 8-20
SSH
鍵の削除 4-32
鍵の生成 4-33
サービス 3-19
設定 3-19
state コマンド 8-23, 13-7
strong
動的フィルタのアクション 7-32
ポリシー アクション 8-31
ユーザ フィルタのアクション 7-25
syn_by_fin パケット タイプ 8-19
syns パケット タイプ 8-19
syslog
エクスポート パラメータの設定 11-9
サーバの設定 11-10
メッセージの形式 11-9

T

TACACS+
検索の設定 4-20
サーバの IP アドレス 4-19
サーバの暗号鍵 4-20
サーバの接続タイムアウト 4-21
サーバの設定 4-18
統計情報の表示 4-22
統計のクリア 4-22

認証
key generate コマンド 4-25, 4-28
tacacs-server コマンド
clear statistics 4-22
first-hit 4-21
show statistics 4-22
timeout 4-22
鍵 4-20
ホスト 4-19
TCP
検出された異常 10-5
ドロップ統計情報 13-11, 13-12
プロキシが使用されない場合のポリシー テンプレート 8-8
ポリシー テンプレート 8-6
thresh-mult 8-27, 13-4, 13-6
threshold
コマンド 8-24
threshold-list 8-28
threshold-selection 6-21
timeout コマンド 8-30
to-user-filters
動的フィルタのアクション 7-32
ポリシー アクション 8-31
traceroute コマンド 11-43
trap 11-9
trap-dest 4-36

U

UDP
unauthenticated ドロップ統計情報 13-11
検出された異常 10-5
ドロップ統計情報 13-11
ポリシー テンプレート 8-7
unauth_pkts パケット タイプ 8-19
upgrade コマンド 12-23
username
暗号化されたパスワード 4-9
username コマンド 4-8

V

VLAN
管理 2-7
スーパーバイザ モジュールへの設定 2-6
設定 3-11
レイヤ 3 インターフェイスの設定 2-8
割り当て 2-7
VPN ルーティングおよび転送、「VRF」を参照
VRF、注入の設定 5-25

W

WBM
アクティブ化 3-18

X

XML スキーマ 10-19 - 10-23, 11-22

Z

zone
コマンド 6-4, 6-7, 9-4
zone-malicious-rate 7-39

あ

アカウンティング、設定　4-17
悪意のあるレートによる終了しきい値　7-38
アクション フロー　10-18
アップグレード
　AP　12-11
　MP　12-14
　インライン　12-17
宛先変更
　アウトオブパスの設定　5-16
　アドバタイズされたルートの表示　5-10, 5-14, 5-21
　インラインの設定　5-11
　概要　5-2
　コマンド　5-8, 5-9
　注入　5-8, 5-23
　定義　5-3
　トラブルシューティング　13-3
　ネットワーク設定　5-3
　ハイジャック　5-7
　メカニズム　5-5
アドバタイズされたルート、表示　5-10, 5-14, 5-21
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　10-5
　フロー　10-13
イベント ログ　11-8
インターフェイス
　IP アドレスの設定　3-9 - 3-12
　アクティブ化　3-8, 3-10
　コマンド　3-9, 3-11, 3-12
　ループバック　3-12
インタラクティブ
　動作モード　9-4
　ポリシーのステータス　8-33
インタラクティブ保護モード　1-7, 6-38
インライン アップグレード　12-17

え

エクスポート
　設定ファイル　12-2
　レポートを自動的に　10-19
　ログ ファイル　11-11

お

オンデマンド　6-45

か

カウンタ
　履歴　11-4
カウンタ、表示　11-4
監視
　ネットワーク トラフィック　11-14, 11-22, 11-23
管理
　SSH　3-19
　VLAN　2-5

WBM 3-18
概要 3-18
ポート 2-5, 3-8, 3-9

き

基本
保護モジュール 8-18
基本保護モジュール 1-9, 8-18
キャプチャ、パケット 11-19
強化
保護モジュール 1-9, 8-18
強化保護モジュール 8-18

く

クライアント攻撃 10-15
クライアント攻撃（軽減された攻撃） 10-9

け

軽減された攻撃
概要 10-6
クライアント攻撃 10-9
スプーフィング利用 10-7
ゾンビ 10-7
不正な形式のパケット 10-11
ユーザ定義 10-10
警告
記号の概要 xxix
検出された
異常 10-5
フロー 10-17

こ

公開鍵
表示 4-33
攻撃のタイプ
クライアント 10-9
軽減された攻撃 10-15
スプーフィング利用 10-7
ゾンビ 10-8, 10-11
不正な形式のパケット 10-11
ユーザ定義 10-10
攻撃の統計情報 13-9
攻撃レポート
dropped/replied packets 10-4
エクスポート 10-19
エクスポート、自動的に 10-19
軽減された攻撃 10-6
検出された異常 10-5
コピー 10-19, 10-20
タイミング 10-3
統計情報 10-3
表示 10-14, 13-8
レイアウト 10-2
コマンドのショートカット 3-7
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
copy 8-44
アクセス権 4-3
イネーブル化 4-3

削除　8-16
追加　8-15
サービスのイネーブル化　4-3
サブゾーン　6-42

し

しきい値
悪意のあるレートによる終了　7-38
受け入れ前の乗算　8-26
固定値として設定　8-25
乗算　13-4, 13-6
選択　8-39
調整　1-6, 6-14
調整済みのマーク付け　6-10, 6-27
特定の IP の設定　8-28
フィルタ レートによる終了　7-38
シグニチャ
生成　11-28
シグニチャの生成　11-28
シグニチャの抽出　11-28
時刻、設定　4-30
自動保護モード　1-7, 6-38
冗長性　2-14, 2-15

す

推奨事項
アクティブ化　9-4, 9-9
受け入れ　9-10
概要　9-2
決定の変更　8-32
コマンド　9-9
通知の受信　9-2
非アクティブ化　9-4
表示　9-2, 9-5
保留フィルタの表示　9-8
無視　9-10
スーパーバイザ モジュール
VLAN の設定　2-6
サポートされているバージョン　12-8
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　2-2
電源の切断　2-12
ブート　2-12
リセット　2-11
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　8-39
比較　8-41
表示　8-42
ポリシーのバックアップ　6-15, 8-40
スプーフィングを利用した攻撃　10-7, 10-15

せ

設置
確認　2-3
設定
スーパーバイザへの保存　2-2

ファイル
インポート 12-4
エクスポート 12-2
コピー 12-2
表示 11-2
設定コマンド 3-8

そ

ゾーン
IP アドレス 6-9
IP アドレスの変更 6-10
LINK テンプレート 6-17
オフラインでの同期 6-33
コピー 6-7
再設定 6-9
削除 6-6
作成 6-4
サブ 6-42
ステータスの表示 11-3
設定の同期 6-30
設定の表示 6-12
設定モード 6-9
定義 1-4, 6-2
テンプレート 6-5
動作モード 6-5
比較 8-42
複製 6-7
フローのブロッキング 13-3
ブロッキング基準 13-5
保護 6-35
ポリシーの表示 8-34
ラーニング 6-13
ゾーンのポリシー
調整済みのマーク付け 6-10, 6-27
その他のプロトコル
検出された異常 10-5
ゾンビ 10-15
パケット カウンタ 11-5
ゾンビ攻撃 10-7, 10-17

た

高いアベイラビリティ 2-15
断片化
検出された異常 10-5

ち

注意
記号の概要 xxviii
注入
VRF 5-25
注入、トンネル 5-29

て

デフォルト設定、～に戻す 12-23
テンプレート
LINK 6-17
ゾーン 6-5
ポリシーの表示 6-7

と

動的フィルタ　7-2
　アクション　7-32
　概要　7-31
　コマンド　7-33, 7-37
　削除　7-37, 13-6
　終了　7-39
　ソート　7-34
　ゾーンの悪意のあるレート　7-39
　定義　1-8
　非アクティブ化　7-38, 13-7
　表示　7-34, 13-5
　防止、作成　7-38
動的フィルタのアクションのブロック　7-32
特定の IP しきい値　8-28
特権レベル　3-2
　～間の移動　4-13
　パスワードの割り当て　4-13
トラフィック
　監視　11-14, 11-22, 11-23
トラフィックのキャプチャ　11-14
トラフィックの記録　11-14
ドロップ
　統計情報　13-10
ドロップされたパケット
　攻撃レポート　10-4
　ラーニング　6-15
ドロップ保護モジュール　1-9

に

認可、設定　4-11, 4-12
認識保護モジュール　1-9
認識モジュール　11-35
認証、設定　4-7
認証されていない TCP の検出された異常　10-6

は

バークリー パケット フィルタ　7-15
バージョン、アップグレード　12-23
バイパス フィルタ
　コマンド　7-21
　削除　7-23
　設定　13-7
　定義　1-8, 7-2
　表示　7-22
ハイブリッド　10-15
パケット、キャプチャ　11-19
パスワード
　暗号化された　4-9
　イネーブル化　4-13
　復旧　12-23, 12-24
　変更　4-10
パスワード、復旧　12-24

ふ

フィルタ
　概要　7-2
　動的　1-8, 7-2, 7-31
　バイパス　1-8, 7-21
　フレックスコンテンツ　1-8, 7-7
　ユーザ　1-8, 7-24

フィルタ レート
終了しきい値 7-39
複数の Guard
設定 2-14
不正な形式のパケット 10-15
軽減された攻撃 10-11
フラッシュの焼き付け 12-21
フレックスコンテンツ フィルタ
設定 7-8
定義 1-8, 7-2
デフォルト設定 11-49
ドロップされた 13-10
番号変更 7-8
表示 7-18
フレックスコンテンツ フィルタの番号変更 7-8
プロキシ
設定 3-17
プロキシが使用されない場合のポリシー テンプレート 8-8
プロキシが使用されない場合のポリシー テンプレート 8-8
分析保護モジュール 1-9, 8-18

へ

返送されたパケット 10-4

ほ

ポート
管理 3-8, 3-9
データ 3-8, 3-9
ポート スキャン
検出された異常 10-5
ポリシー テンプレート 8-6
保護
アクティブ化 3-17
インタラクティブ モード 1-7, 6-38
オンデマンド 6-45
コマンド 6-36
自動的な非アクティブ化 6-43
自動モード 1-7, 6-38
特定の IP 6-37
非アクティブ化 6-38
保護の非アクティブ化 6-43
保護モジュール
「モジュール」を参照
ホスト、ロギング 11-10
ホスト鍵
削除 4-28
ポリシー
copy-policies 8-44
learning-params fixed-threshold コマンド 8-25
アクション 8-22, 8-31
アクティブ化 8-22
現在の～のバックアップ 6-15, 8-40
構造 8-2
構築 1-6, 6-14, 6-17, 8-4
コマンド 8-21
サービスの削除 8-16
サービスの追加 8-15
しきい値 8-4, 8-22, 8-24
しきい値の乗算 8-27, 13-4, 13-6
しきい値の調整 1-6, 6-14, 6-19

しきい値を固定　8-25
状態　8-22
タイムアウト　8-22, 8-30
調整、しきい値　8-4
調整済みのマーク付け　6-10, 6-27
ディセーブル化　8-22
統計情報の表示　6-23, 8-36
トラフィック特性　8-20
ナビゲーション パス　8-21
パケット タイプ　8-18
パラメータのコピー　8-44
非アクティブ化　8-22
表示　13-6
プロキシしきい値　8-29
ポリシー テンプレート
max-services　8-10
min-threshold　8-11
概要　8-5
コマンド　8-8, 8-9, 8-12
状態　8-11
設定コマンド レベル　8-9
パラメータ　8-9
ポリシーの構築　6-17
ポリシーのしきい値の調整　6-19
保留動的フィルタ　9-2
表示　9-8

め

メモリ消費量　11-35
メンテナンス パーティション
「MP」を参照

も

モジュール
概要　8-18
基本　1-9, 8-18
強化　1-9, 8-18
ドロップ　1-9
認識　1-9, 11-35
分析　1-9
レート リミット　1-9, 7-21
分析　8-18

ゆ

ユーザ
Admin　2-9
riverhead　2-9
新しい～の追加　4-8
検出された異常　10-6
削除　4-9
追加　4-8
特権レベル　3-2, 4-12
特権レベルの割り当て　4-8
ユーザ定義（軽減された攻撃）　10-10
ユーザ フィルタ
アクション　7-25
コマンド　7-8, 7-26
削除　7-29
設定　7-24
定義　1-8, 7-2
番号変更　7-26
表示　7-28
ユーザ フィルタの番号変更　7-26

ら

ラーニング
　概要　6-13
　結果の同期　6-16
　しきい値の調整　6-19
　ドロップされたパケット　6-15
　プロセスの終了　6-19, 6-22
　ポリシーの構築　6-17

り

リブート
　パラメータ　12-7

る

ルーティング テーブル
　操作　3-15
　表示　3-16
ループバック インターフェイス　3-12

れ

レイヤ 3 インターフェイス
　VLAN への設定　2-8
レート、表示　11-4
レート リミット保護モジュール　1-9, 7-21
レポート
　「攻撃レポート」*を参照*　10-2
　詳細　10-14

ろ

ロード シェアリング　2-14
ロギング、設定の表示　11-10
ログ ファイル
　エクスポート　11-8, 11-11
　クリア　11-12
　表示　11-11