

Cisco Anomaly Guard モジュール

Cisco® Anomaly Guard モジュールは、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに搭載するサービス モジュールで、大規模な Distributed Denial of Service (DDoS; 分散型サービス拒否) 攻撃からオンライン リソースを保護する強力で幅広いソリューションを提供します。Cisco Anomaly Guard モジュールは、大規模企業やサービス プロバイダーの環境で求められる要求の厳しいパフォーマンス要件とスケーラビリティ要件を満たし、複雑さと巧妙さが増大する攻撃からネットワークを確実に保護します。

Cisco Anomaly Guard モジュール(図 1)は、モジュールあたりマルチギガビットのライン レートで攻撃トラフィックを処理します。独自の「オンデマンド」展開モデルを利用すると、他のトラフィックに影響を与えることなく対象となるデバイスまたはゾーン宛のトラフィックのみを迂回処理させることができます。Cisco Anomaly Guard モジュールでは、モジュール内に統合された多層構造の防御機能によって不正な攻撃トラフィックの識別とブロックが行われ、正規のトランザクションは引き続き元の宛先に転送されます。攻撃を受けているときでも、業務の運用が中断されることはありません。

図 1 Cisco Anomaly Guard モジュール



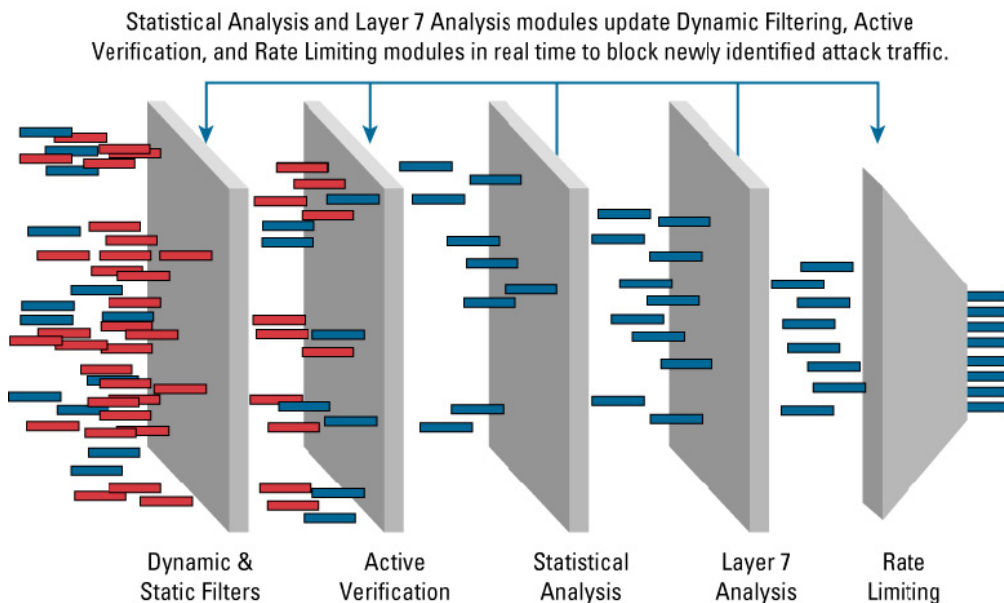
1 台のシャーシで複数の Cisco Anomaly Guard モジュールを使用すると、モジュールの数だけ処理能力が向上するため、大規模または業務拡張中の企業やサービス プロバイダーの環境にも対応でき、拡張性に富んだソリューションを実現できます。Cisco Anomaly Guard モジュールのマルチプロセッサ アーキテクチャは、さらに大規模な攻撃にも対応可能な防御力を拡張するためのライセンス付きソフトウェアの将来的なアップグレードもサポートしています。

進化する DDoS 攻撃

最近の DDoS 攻撃は、壊滅的な打撃をもたらし、以前よりも目的が明確化されています。DDoS 攻撃は、一般的な防御策を施したとしても簡単に回避または突破されてしまいます。DDoS 攻撃では、正規の要求の模倣、大量のゾンビ ホストの使用、ID のなりすましなどが行われるため、不正なフローを識別して阻止することはほとんど不可能です。DDoS 攻撃は、企業の業務を麻痺させて妨害することで、取引と顧客の損失から信用の低下と法的責任まで、年間数十億ドルの損失を与えます。

Cisco Anomaly Guard モジュールはあらゆるタイプの DDoS 攻撃からネットワークを防御します。Cisco Anomaly Guard モジュールを使用すると、企業は悪意のあるトラフィックを識別してブロックし、ミッションクリティカルで収益につながる業務への影響を軽減することができます。特許取得済みの独自の多層検証処理アーキテクチャに基づく Cisco Anomaly Guard モジュールは、高度な異常認識機能によって、高性能フィルタリングとともに送信元確認技術およびなりすまし対策をダイナミックに実行し、正規のトランザクションの流れを妨げずに、個々の攻撃フローを識別してブロックします(図 2)。また、使いやすいグラフィカル インターフェイス、マルチレベルの監視拡張機能とレポート拡張機能が備わっているため、すべての攻撃活動を包括的に表示することができます。これらの機能によって Cisco Anomaly Guard モジュールは、パフォーマンスの高い DDoS 防御を実現し、業務を確実に保護します。

図 2 Cisco Anomaly Guard モジュールの多層検証処理アーキテクチャ



Cisco Anomaly Guard モジュールの概要

Cisco Anomaly Guard モジュールは、大企業、行政機関、ホスティング センター、およびサービス プロバイダーなどを DDoS 攻撃から保護するシスコの包括的な検出および攻撃軽減対策ソリューションです。Cisco Anomaly Guard モジュールの強力でスケーラブルなソリューションにより、ホスティング プロバイダーやサービス プロバイダーは加入者に対して優れたマネージド DDoS 保護サービスを提供できます。Cisco Traffic Anomaly Detector モジュール(または DDoS 攻撃を検出するサードパーティ製の警告システム)と併用すると、攻撃に関するフローレベル単位の詳細な分析、識別、および軽減対策サービスを実行して、ネットワークやデータセンター業務への影響を未然に防ぐことができます。

Cisco Traffic Anomaly Detector モジュールが攻撃の可能性を検出すると、Cisco Anomaly Guard モジュールに警告を送り、対象リソース宛のトラフィック(該当するトラフィックのみ)をダイナミックに迂回処理して検査します。その他のすべてのトラフィックは引き続き目的の宛先に転送されるため、ネットワークへの影響が少なく、信頼性と費用対効果の高い、設定の容易なソリューションを実現できます。

迂回処理されたトラフィックは Cisco Anomaly Guard モジュールに再ルーティングされ、詳細な検査を受けて「不正な」フローと正規のトランザクションに分類されます。識別された攻撃パケットは削除されますが、「正規の」トラフィックは元の宛先に転送されます。この処理により、正規のユーザおよびトランザクションは正常に処理され、アベイラビリティを最大限に活かすことができます。

Cisco Anomaly Guard モジュールの利点

多層検証

Cisco Anomaly Guard モジュールの先進的なブロッキング技術は、シスコ独自の多層検証処理アーキテクチャをベースに、インタラクティブな複数の防御層を通じて、すべてのタイプの攻撃を正確に識別してブロックします。高度なプロファイルベースの異常認識エンジンで推進されるダイナミック フィルタリング機能とアクティブな検証技術が統合されたことにより、Day-Zero 攻撃を含め、あらゆるタイプの攻撃がすばやく自動的に防御されます。Cisco Anomaly Guard モジュールはフロー単位の詳細な分析と保護を実行して、正規のトランザクションに影響を与えることなく、不正なトラフィックを外科的な手腕と正確さでブロックします。

異常認識エンジンは、フロー単位の詳細なプロファイルを含む正常動作を基準に、保護対象リソースの正常動作または予測される動作を定義します。必要に応じて、サイト固有の自動学習機能を使用すると、さらに精度の高いデフォルト プロファイルを作成することができます。この自動学習機能は個々のデバイスまたはゾーンのプロファイルをカスタマイズします。

さらに、レート制限機能は、大規模なフラッディングからの防御だけでなく、ブロッキングに代わる軽減対策も実行します。また、スタティック フィルタ、詳細なパケット検査フィルタの作成が可能な Berkeley Packet Filter に基づく Flex フィルタ、およびバイパスの「ホワイトリスト」フィルタも使用できます。

Cisco Anomaly Guard モジュールには、ゾンビと呼ばれる障害のあるコンピュータから仕掛けられるあらゆるタイプと規模の攻撃を打破する「ゾンビ キラー」機能も搭載されています。ゾンビ攻撃は、現在、最も広く蔓延している防御の難しい DDoS 攻撃の 1 つです。Cisco Anomaly Guard モジュールをクラスタ構成で使用すると、文字通り数十万のゾンビを識別し、阻止できるので、大規模なボットネット (botnet) 攻撃からネットワークを確実に防御できます。

マルチギガビット パフォーマンス

Cisco Anomaly Guard モジュールには、攻撃の分析と浄化をフル ギガビット ライン レートで行う専用のネットワーク プロセッサが搭載されているため、広く分散している多数のホスト (ゾンビ ホストなど) からの大規模な DDoS 攻撃を阻止できます。

Cisco Anomaly Guard モジュール ソフトウェア リリース 5.1 以下では、各モジュールは 1 Gbps のスループットでの動作をサポートしていました。リリース 6.0 以降では、Cisco Anomaly Guard モジュールは 3 Gbps のスループットで動作できます。ソフトウェア ライセンスを使用してモジュールで追加のネットワーク プロセッサを稼働させると、より高いパフォーマンスを実現できます。

Cisco Anomaly Guard モジュールは 1 台のシャーシに複数搭載することができ、モジュールの数だけ処理速度 (パケット/秒) とゾンビ攻撃への防御能力が増強します。そのため、大規模な企業やサービス プロバイダーの環境を最も強力な攻撃から確実に保護することができます。また、複数のモジュールをクラスタ化して、単一のリソースやゾーンを保護することもできます。この場合、専用のロード バランサは必要ありません。

10 ギガビット以上のキャパシティへの拡張

Cisco Anomaly Guard モジュール ソフトウェア リリース 6.0 では、各 Cisco Anomaly Guard モジュールが 3 Gbps で動作するため、単一のシャーシで最大 4 つのモジュールをクラスタ処理することで 10 ギガビット以上のパフォーマンスを実現できます。詳細については、下記のパフォーマンスのメトリックに関する表を参照してください。

ダイナミックな迂回機能

Cisco Anomaly Guard モジュールでは、強力なオンデマンド型のスクラビング モデルが使用されています。このモジュールは従来型のインライン デバイスとは異なり、通常のデータ パス上には設置されず、ダイナミックな迂回機能により、攻撃対象のリソースやゾーン宛のトラフィック(該当するトラフィックのみ)を自動的にリダイレクトして詳しく解析します。攻撃が検出されると、Cisco Anomaly Guard モジュールは Cisco Route Health Injection(RHI) プロトコルを使用して、スーパーバイザ エンジンのルーティング テーブルをダイナミックに更新し、Cisco Anomaly Guard モジュールを攻撃対象リソース宛トラフィックのネクストホップにします。

攻撃対象のデバイスやゾーン宛のトラフィックが浄化されて不正パケットがブロックされると、正規のトランザクションは元の宛先に転送されるので、重要な要求が消失することはありません。迂回処理されるトラフィックは、現在攻撃対象となっているリソースやゾーン宛のフローに限定されるため、大規模な企業やサービス プロバイダーの環境要件に最適なリソース稼働率、透過性、信頼性を備えた拡張性の高いソリューションを実現できます。このようにレイヤ 3 機能を追加する方式は、設置時に生じるネットワークへの影響が少なく、設置自体も簡単です。また、運用管理とトラブルシューティングも容易に行えます。

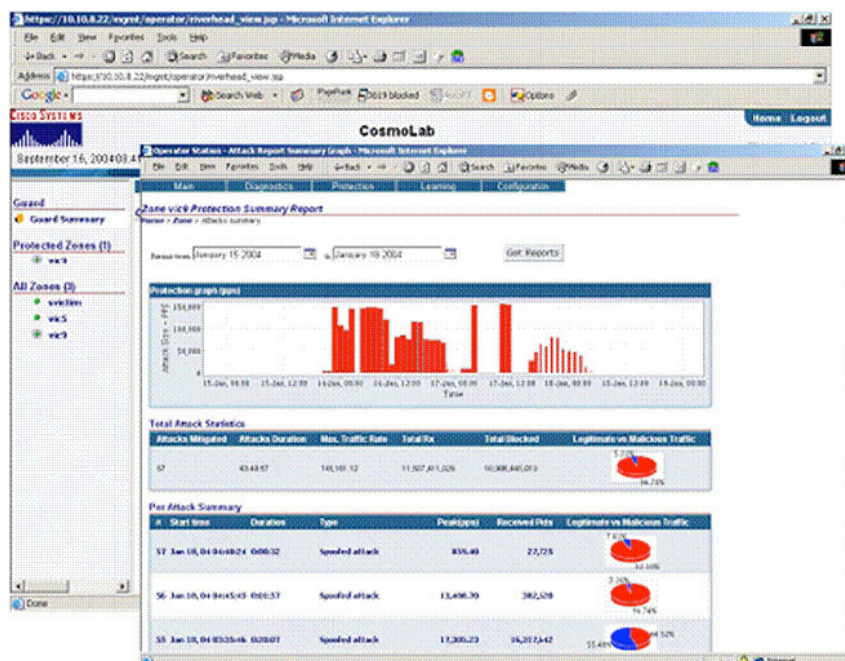
マルチレベルの監視機能とレポート機能

Cisco Anomaly Guard モジュールは、使いやすい Web ベースの GUI を備えているため、ポリシー定義、動作監視、およびレポート生成の処理が簡素化されます。

ネットワーク オペレータ、セキュリティ管理者、およびクライアントは、マルチレベルの監視機能とレポート機能を使用して、詳細なリアルタイム情報や履歴情報を入手できます(図 3)。攻撃レポートでは、個々の攻撃に関する詳細な情報(攻撃の特性、識別されたゾンビ リスト、および実行された処置など)が提供されるため、セキュリティ担当者は Cisco Anomaly Guard モジュールのセキュリティ ポリシーをレビューし、調整することができます。

また、カスタマーレベルの履歴サマリーを使用すると、サービス プロバイダーは攻撃の種類、時間、および規模など防御実績に関するレポートを容易に作成できます。さらに、インタラクティブ モードを使用すると、ユーザは推奨処置やポリシーの承認を行う前に、これらをレビューすることができるため、攻撃への対処方法を必要に応じて手動で管理できます。

図 3 マルチレベルの監視機能とレポート機能により、リアルタイムのパフォーマンスとパフォーマンス履歴を詳細に把握することが可能



Cisco Anomaly Guard モジュールのパフォーマンス メトリック

表 1 に、Cisco Anomaly Guard モジュールのパフォーマンスとキャパシティの詳細を示します。

表 1 Cisco Anomaly Guard モジュールのパフォーマンスとキャパシティ

機能	説明
パフォーマンス	<p>オプション 1 : 1 Gbps</p> <ul style="list-style-type: none"> モジュールあたり 1 Gbps のスループット 最大 150,000 のダイナミック フィルタ 150 万の同時接続 500 の保護ゾーン(異なるポリシーと基準 [コンテキスト]) 30 のゾーンを同時に保護 1 ミリ秒未満の遅延とジッタ <p>オプション 2: 3 Gbps</p> <ul style="list-style-type: none"> モジュールあたり 1 Gbps のスループット 最大 150,000 のダイナミック フィルタ 450 万の同時接続 500 の保護ゾーン(異なるポリシーと基準 [コンテキスト]) 50 のゾーンを同時に保護 1 ミリ秒未満の遅延とジッタ
クラスタ処理	<p>オプション 1: 1 Gbps モジュールのクラスタ処理</p> <ul style="list-style-type: none"> 等コスト マルチパス ルーティングを使用 専用ロード バランサは不要 Cisco Catalyst 6509/Cisco 7609 シャーシで最大 6 モジュール Cisco Catalyst 6513/Cisco 7613 シャーシで最大 10 モジュール <p>オプション 2: 3 Gbps モジュールのクラスタ処理</p> <ul style="list-style-type: none"> 等コスト マルチパス ルーティングを使用 専用ロード バランサは不要 Cisco Catalyst 6509/Cisco 7609 シャーシで最大 6 モジュール Cisco Catalyst 6513/Cisco 7613 シャーシで最大 10 モジュール

Cisco Anomaly Guard モジュールの全体的な機能の概要

表 2 に、Cisco Anomaly Guard モジュールの機能を示します。

表 2 Cisco Anomaly Guard モジュールの機能

機能	説明
攻撃への防御	<ul style="list-style-type: none"> なりすまし攻撃および非なりすまし攻撃 TCP (SYN、SYN-ACK、ACK、FIN、フラグメント) 攻撃 UDP 攻撃(ランダム ポート フラッド、フラグメント) Internet Control Message Protocol (ICMP) 攻撃(到達不能、エコー、フラグメント) Domain Name System (DNS; ドメイン ネーム システム) 攻撃 クライアント攻撃 非アクティブおよび Total Connections 攻撃 HTTP Get フラッド攻撃 Border Gateway Protocol (BGP) 攻撃 Session Initiation Protocol (SIP) Voice over IP (VoIP) 攻撃
継続的なラーニングと保護	<ul style="list-style-type: none"> ラーニングおよび保護モードで継続的に稼働可能(リリース 5.0 以上) しきい値の調整と攻撃からの保護を同時に実行 ラーニングと保護モード間の切り替えは自動 攻撃の収束後ラーニング モードに戻る
トラフィックの分析	<ul style="list-style-type: none"> モジュールを通過するパケットをキャプチャし pcap ファイルとして保存 GUI によりキャプチャしたパケットを詳しく分析 キャプチャの対象を特定の決定値(転送、廃棄、応答)を持つパケットに限定可能 tcpdump 式を使用してキャプチャをフィルタ可能
シングニチャの抽出 — ディープ パケット インスペクション	<ul style="list-style-type: none"> キャプチャしたパケットのペイロードの顕著なパターンを検出 自動アルゴリズムによりキャプチャしたパケットを分析し、不正なパケットにだけみられるシングニチャを抽出 コンテンツベースのフィルタを抽出したシングニチャに適用可能
コンテンツベース フィルタ	<ul style="list-style-type: none"> ペイロード内のパターンを検索 複数のコンテンツベース フィルタを定義可能 パケットのカウントのみか、廃棄するかを設定可能

機能	説明
通信プロトコル	<ul style="list-style-type: none"> Secure Shell (SSH)、Secure Sockets Layer (SSL)、File Transfer Protocol (FTP); ファイル転送プロトコル)、Secure FTP (SFTP)
管理	<ul style="list-style-type: none"> CLI (コマンドライン インターフェイス) コンソール CLI への SSH アクセス Cisco Guard Device Manager への SSL アクセス Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) MIB、MIB II、およびトラップのサポート
Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントING) のサポート	<ul style="list-style-type: none"> TACACS+ による AAA との統合 特権レベルおよびコマンドレベルの許可とアカウントING
セキュリティ	<ul style="list-style-type: none"> 管理インターフェイス上の IP テーブルと DDoS 攻撃への自己防衛
ロギング	<ul style="list-style-type: none"> 包括的な Syslog 機能およびイベント

構成および展開オプション

Cisco Anomaly Guard モジュールには、統合モードと専用モードの 2 つの異なる展開オプションが用意されています。

統合モードの場合、1 つまたは複数の Cisco Anomaly Guard モジュールが既存の Cisco Catalyst 6500 シリーズまたは Cisco 7600 シリーズ シャーシ (データセンター内に展開され、通常のレイヤ 3 データ パス上に存在) に搭載されます。攻撃が検出されると、疑いのあるトラフィックは Cisco Catalyst バックプレーン経由で Anomaly Guard モジュールにダイナミックに迂回処理され、解析と駆除のあと、次のダウンストリーム デバイスに転送されます。

専用モードの場合、専用の Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに Cisco Anomaly Guard モジュールを搭載します。この構成では、複数の Cisco Anomaly Guard モジュールをクラスタ化して大規模な保護を実現します。専用モードで攻撃が検出されると、サポートされている Cisco IOS[®] ソフトウェアのルーティング プロトコルにより、疑わしいトラフィックはアップストリーム スイッチまたはルータから専用の Cisco Catalyst スイッチへと転送されます。専用シャーシ内の Cisco Anomaly Guard モジュールは、スーパーバイザ エンジンのルーティング プロセスによって転送されたトラフィックのネクストホップになります。転送されたトラフィックは Cisco Anomaly Guard モジュールで解析され、不正なトラフィックは削除されます。正規のトラフィックは Cisco Anomaly Guard モジュールによってネットワークに戻され、元の宛先に転送されます。

また、Cisco Traffic Anomaly Detector モジュールも統合モードまたは専用モードのいずれかで設置できますが、監視対象トラフィックのコピーを受信するために、(ルーティングに対して) 1 段階または 2 段階のバケットキャプチャ処理を要求します。

統合モードまたは専用モードのいずれの場合でも、攻撃が検出された場合、Cisco Anomaly Guard モジュールはアクティブ化され、迂回処理を開始できるようになります。この場合、Cisco Anomaly Guard モジュールは、Cisco Catalyst シャーシ内で Cisco RHI プロトコルを使用して、スーパーバイザ エンジンのルーティングをダイナミックに更新し、Cisco Anomaly Guard モジュールをネクストホップにします。専用モードの場合、通常、アップストリーム デバイスにルートの更新を再配布するようにスーパーバイザ エンジンの設定が行われます。その他の迂回処理方法には、オペレータによるルート更新の指定や永続的なスタティック ルートなどがあります。

使用例

シスコの DDoS 異常検出および軽減対策ソリューションは、企業およびサービス プロバイダーのさまざまなトポロジで利用できます (図 4 ~ 6)。

図 4 企業またはホスティング データセンターにおけるシスコの DDoS 異常検出および軽減対策

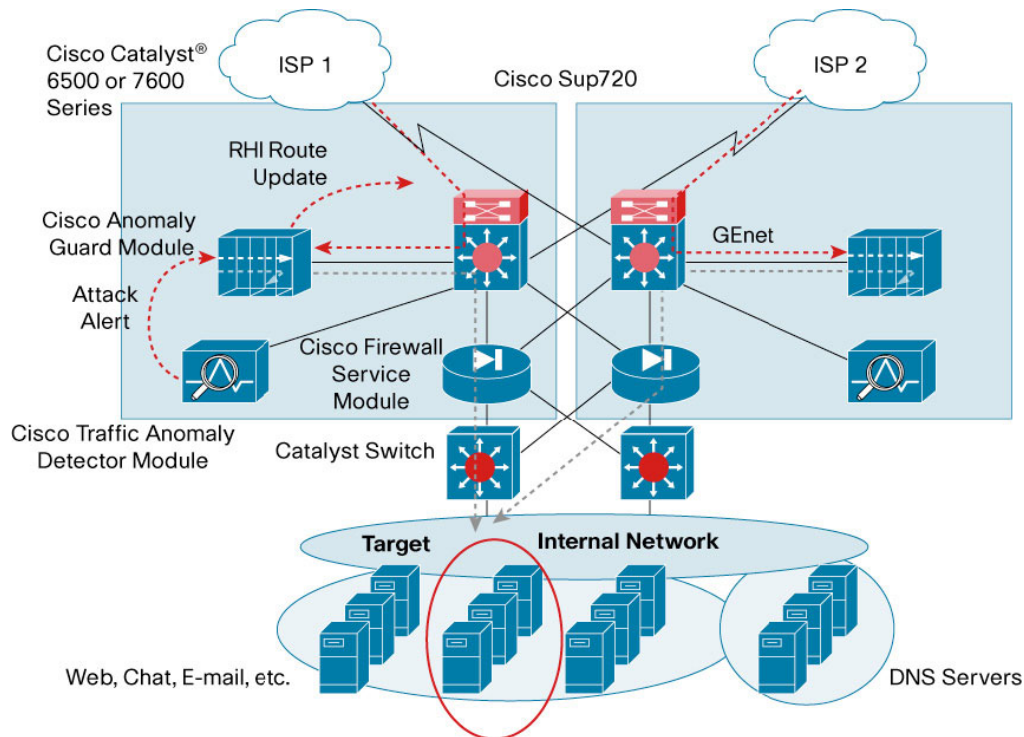


図 5 サービス プロバイダー環境における DDoS の分散型/エッジ保護

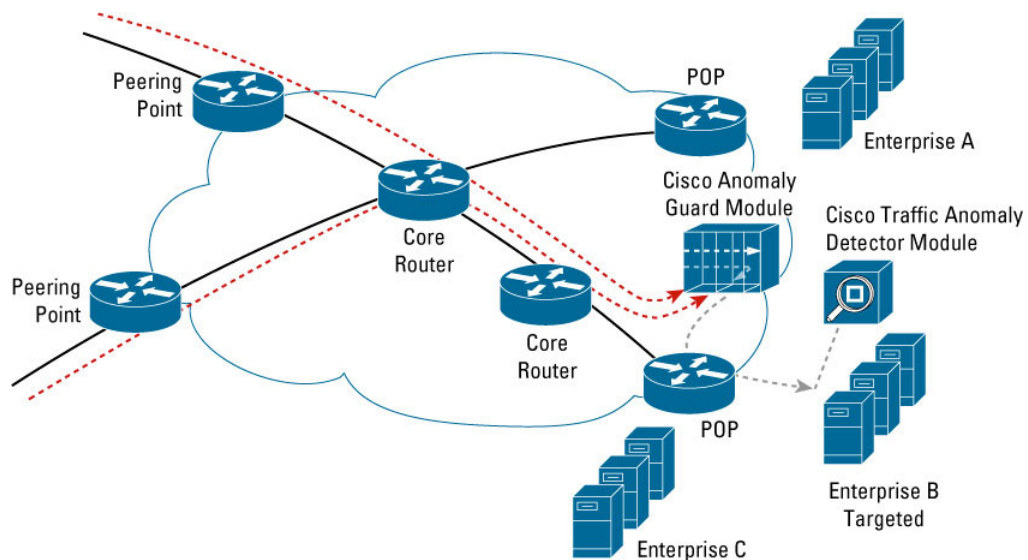
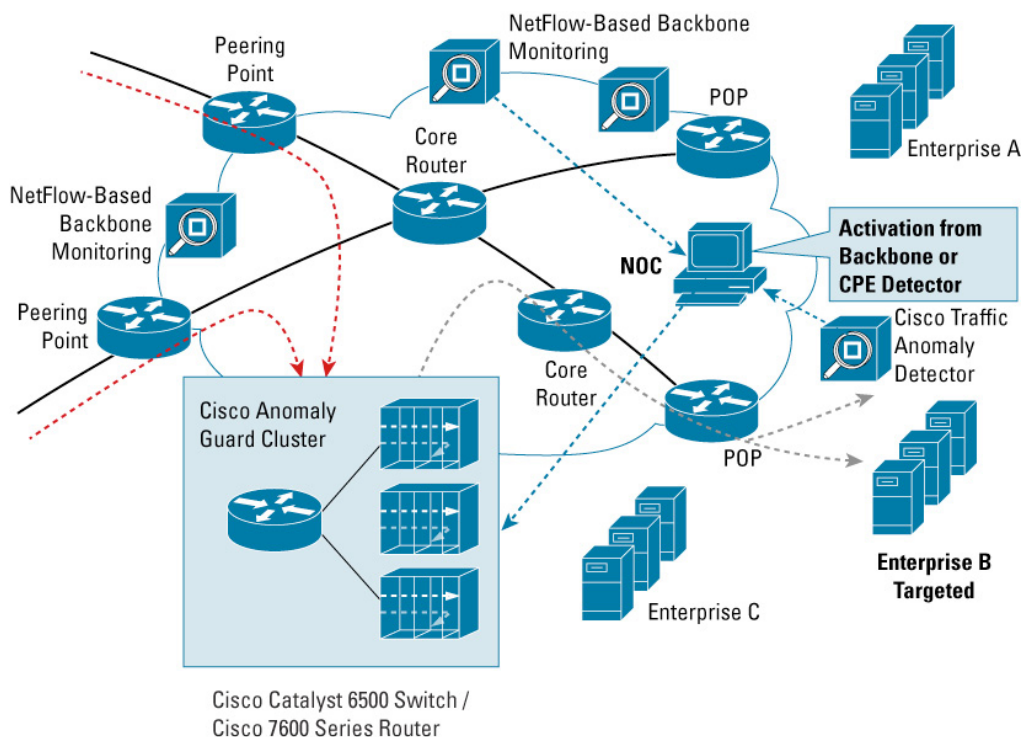


図 6 サービス プロバイダーのスクラビング センター内におけるシスコの DDoS 異常検出および軽減対策



セキュリティ サービスの統合化による利点

セキュリティ サービスの統合

Cisco Anomaly Guard モジュールは、Firewall Services Module (FWSM)、Intrusion Detection Services Module (IDSM-2)、Content Switching Module (CSM)、Network Analysis Module (NAM-1 および NAM-2) などの他のシスコ セキュリティ サービス モジュールと組み合わせることができます。これらのサービス モジュールを一緒に使用すると、完全な自己防衛型ネットワーク ソリューションを実現できます。

柔軟性のある展開

Cisco Anomaly Guard モジュールを、Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ内に搭載すると、DDoS 保護機能のすべてがネットワーク インフラストラクチャと統合されます。モジュールは既存のスイッチやルータに容易に搭載できるため、インターフェイス ポートを使用することなく、必要なときに必要な場所で強力な DDoS 保護サービスを使用できます。また、DC 電源、Network Equipment Building Standards (NEBS) などの可用性に優れたオプションを使用して、高密度専用スクラビング アプライアンスやマルチサービス セキュリティ スイッチを、さまざまなサイズのシャーシで展開することもできます。ライン カードは相互運用可能なので、媒体を柔軟に使用できます。迂回機能は完全にシャーシ内で実行するか、または、Cisco IOS ソフトウェアのスーパーバイザ エンジンに搭載されたルーティングおよびトンネリング プロトコルのサポートをフルに活用して複数のデバイスで実行できます。

スケーラビリティ

大容量の保護が必要な場合は、1 台のスイッチに 8 つのモジュールを搭載して、大規模で急速に拡大する環境に対応します。また、Cisco Anomaly Guard モジュールのマルチプロセッサ アーキテクチャとマルチギガビットのバックプレーン インターフェイスは、ライセンス付きソフトウェアの将来的なアップグレードを、モジュールあたり数ギガビットのパフォーマンスまでサポートしています。

信頼性とハイ アベイラビリティ

Cisco Anomaly Guard モジュールは、ルーティングベースのダイナミックな迂回処理機能と強固なフェールオーバー保護機能を備えた強力なオンデマンド スクラビング アーキテクチャを保持しています。この機能により、導入が簡素化され、運用面における信頼性が向上し、トランスペアレントな動作が可能となっています。従来のインライン ソリューションでは、アクティブな軽減対策サービスに必要とされるこれらの機能を実現することは不可能でした。Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータでは、DDoS に対抗するためのコントロール プレーン ポリシングと可用性の高い各種オプションも提供されています。

所有コストの削減

これらのモジュールは、他のサービス モジュールとともに Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに搭載されるため、管理対象デバイスの数と運用コストが削減されます。また、モジュールのアプリケーション ソフトウェアとアプライアンスのアプリケーション ソフトウェアは類似しているため、習得にかかる費用を最小限に抑えることができます。モジュールを利用することで、ユーザは既存のスイッチングやルーティング インフラストラクチャを使用できるため、費用対効果の高い環境を実現できます。同時に、業界で最高のパフォーマンスを発揮するとともに、安全な IP サービスとマルチレイヤ LAN/WAN スwitching/ルーティング機能を提供することができます。

まとめ

サービス プロバイダー、ホスティング センター、オンライン企業用に設計された Cisco Anomaly Guard モジュールは、競合他社には実現できない卓越した DDoS 軽減対策ソリューションを提供し、最も悪質な攻撃のさなかにあってもビジネスの流れを妨害させません。これにより、企業は大きな競争力を獲得して、最も価値の高いビジネス資産を最大限に活かし、比類のない防御力を身につけることができます。

システム要件

- Cisco Anomaly Guard モジュール ソフトウェア リリース 5.0 以降
- 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) が搭載された Cisco Catalyst 6500 シリーズ Supervisor Engine 2 または Cisco Catalyst 6500 シリーズ Supervisor Engine 720 (Cisco Catalyst 6500 シリーズ Supervisor Engine 1 はサポート対象外)
- Supervisor Engine 2 の Switch Fabric Module (SFM) (1 Gbps を超えるトラフィックを処理する場合)
- VPN Routing and Forwarding (VRF) を使用して、スーパーバイザ エンジンに対して正規トラフィックを戻すように設定する場合、Multiprotocol Label Switching (MPLS; マルチプロトコルラベル スwitching) に対応した Supervisor Engine 720 モジュール (WS-SUP720-3B または WS-SUP720-3BXL) が必要
- ネイティブの Cisco IOS ソフトウェア リリース 12.2(18)SXD3 以降。Cisco 7600 シリーズ ルータを使用する場合、正式なサポートの対象となるのは Cisco IOS ソフトウェア リリース 12.2(18)SXE 以降
- Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータのスロットを 1 つ 使用
- シャーシあたり最大 8 つの Cisco Anomaly Guard モジュールが使用可能 (同じ宛先を分散モードで保護する場合、またはさまざまな宛先を保護する場合)。同じシャーシ内で Cisco Anomaly Guard モジュールと Cisco Traffic Anomaly Detector モジュールを使用する場合、合計 8 つのモジュールの併用が可能。標準以外の構成でインストールする場合は、リリース ノートを参照するか、またはシスコのテクニカル サポート担当者に相談してください。

- 冗長スーパーバイザ エンジン は Stateful Switchover (SSO; ステートフル スイッチオーバー) モードの Nonstop Forwarding (NSF; ノンストップ フォワーディング) で使用することが必要 (Route Processor Redundancy [RPR] または RPR+ の場合は不要)

製品仕様

表 3 に、Cisco Anomaly Guard モジュールの製品仕様を示します。

表 3 製品仕様

仕様	説明
メモリ	7 GB DDRAM、1 GB コンパクト フラッシュ
重量	<ul style="list-style-type: none"> 最小: 1.36 kg (3 ポンド) 最大: 2.27 kg (5 ポンド)
高さ	40 mm (1.6 インチ)
幅	379 cm (15.3 インチ)
奥行	403 cm (16.3 インチ)
動作温度	0 ~ 40°C (32 ~ 104°F)
保管温度	-40 ~ 75°C (-40 ~ 167°F)
湿度	10 ~ 90% (結露しないこと)
管理機能	<ul style="list-style-type: none"> 安全な Web ベースの GUI CLI (コンソール、Telnet、SSH) Cisco (Riverhead) SNMP MIB および MIB II TACACS+ Syslog
認定	<ul style="list-style-type: none"> UL 認定 CE FCC パート 15 との適合性

発注情報

表 4 に、Cisco Anomaly Guard モジュールの発注情報を示します。

表 4 発注情報

製品名	製品番号
Cisco Catalyst 6500 シリーズ/Cisco 7600 シリーズ Anomaly Guard モジュール	WS-SVC-AGM-1-K9
Cisco Catalyst 6500 シリーズ/Cisco 7600 シリーズ Anomaly Guard モジュール (スペア)	WS-SVC-AGM-1-K9=
Cisco Catalyst 6500 シリーズ/Cisco 7600 シリーズ Anomaly Guard モジュール ソフトウェア リリース 5.1	SC-AGM-5.1-K9
Cisco Catalyst 6500 シリーズ/Cisco 7600 シリーズ Anomaly Guard モジュール ソフトウェア リリース 6.0 1G	SC-AGM-6.0-1G-K9
Cisco Catalyst 6500 シリーズ/Cisco 7600 シリーズ Anomaly Guard モジュール ソフトウェア リリース 6.0 3G	SC-AGM-6.0-3G-K9
Cisco Catalyst 6500 シリーズ/Cisco 7600 シリーズ Anomaly Guard モジュール ソフトウェア リリース 6.0 3G ライセンス	LIC-AGM-3G-K9

シスコ製品の購入方法の詳細は、[「発注方法」](#)を参照してください。

テクニカル サポート サービス

企業規模、業態、またはサービス プロバイダーであるか否かを問わず、シスコはお客様のネットワークへの投資を最大限に活かせるようサポートします。シスコでは、シスコ製品の効率的な運用、ハイアベイラビリティの維持、および最新のシステム ソフトウェアの活用を支援するための豊富なテクニカル サポート サービスを用意しています。

シスコのテクニカル サポート サービス部門は、以下に挙げるサービスを提供しています。これらのサービスを利用すると、ネットワークへの投資を保護し、ミッションクリティカルなアプリケーションが稼働しているシステムの停止時間を最小限に抑えることができます。

- シスコのネットワーキング技術をオンラインおよび電話で提供します。
- 不具合が発生した場合の対応だけでなく、ネットワークの運用に不可欠なソフトウェアのアップデートとアップグレードによるプロアクティブなサポート体制を用意しています。
- 必要に応じてシスコの専門知識とリソースをご利用いただけます。
- お客様の技術スタッフのリソースを補強して、生産性を向上させます。
- 遠隔地のテクニカル サポートでは、オンサイトのハードウェア交換を実施します。

シスコのテクニカル サポート サービスには、次の内容が含まれます。

- Cisco SMARTnet[®] サポート
- Cisco SMARTnet オンサイト サポート
- Cisco Software Application Services (Software Application Support [SAS] および Software Application Support plus Upgrades [SASU] など)

サポート サービスについての詳細は、以下の URL を参照してください。

<http://www.cisco.com/jp/services/>

関連情報

Cisco Anomaly Guard モジュールの詳細については、

<http://www.cisco.com/jp/product/hs/ifmodule/csm/agm/index.shtml> をご覧ください。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00