

Cisco Guard XT 5650



製品概要

シスコシステムズの Cisco® Guard XT 5650 DDoS 軽減対策アプライアンスは、Distributed Denial of Service (DDoS; 分散型サービス拒否) 攻撃からネットワークを保護するための強力な包括的なシステムを実現します。Cisco Guard XT は、最も要求の厳しい各種サービス プロバイダー、大企業、政府機関、教育・研究機関のネットワーク環境におけるパフォーマンスおよびスケラビリティ要件を満たすように設計されており、ますます複雑化して原因を突き止めにくなっている最新の攻撃に対応できる、最高レベルの保護機能を提供します。

Cisco Guard XT には、1 台あたり 2 つのギガビット イーサネット インターフェイスが装備されており、Gbps (ギガビット/秒) というライン レートで攻撃トラフィックを処理できます。複数の Cisco Guard XT を連携させれば、マルチギガビット レートをサポートするように段階的に拡張できるため、拡大する大規模なネットワーク環境に拡張性のあるソリューションをもたらします。

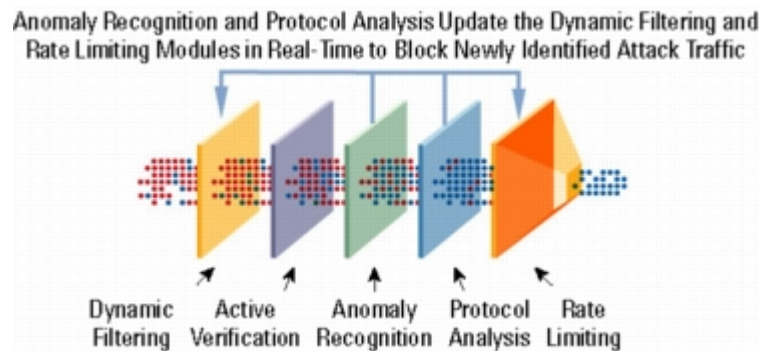
巧妙化が進む DDoS 攻撃

現在の DDoS 攻撃は、かつてなく悪質化し、感染力も強くなってより破壊的になっているため、多くの関心を集めています。不満を持つユーザや良心のないユーザ企業などが特定のサイトや競争相手を標的にして DDoS 攻撃を仕掛けています。こうした攻撃は、最も一般的な防御対策を簡単にかわし、機能を停止させてしまいます。適正を装った要求、多数の「ゾンビ」、および偽造された ID などを利用する DDoS 攻撃は、悪意のあるフローの識別とブロックを事実上不可能にすることで、ターゲットを麻痺させて業務を停滞させ、年間数十億ドルもの収益減をもたらします。

Cisco Guard XT を導入することで、サービス プロバイダー、企業、政府機関、教育・研究機関のネットワーク システムでは、この DDoS 攻撃の新しい波に対抗し、収益を生み出すミッションクリティカルな活動を損なうことなく DDoS 攻撃を撃退できます。独自の Multiverification Process (MVP) アーキテクチャに基づいた Cisco Guard XT では、先進の異常識別、送信元検証、およびスプーフィング防止技術を利用し、個々の攻撃フローを識別してブロックする一方、適正なトランザクションの通過は許可します。Cisco Guard XT には、わかりやすい GUI (グラフィカル ユーザ インターフェイス) と、すべての攻撃活動の概要を把握できるように設計されたマルチレベルのモニタリ

ングおよびレポート機能が装備されています。これらの機能により、強力で包括的な DDoS 防御を提供して業務を保護します。

図 1 Cisco Guard XT の MVP アーキテクチャ



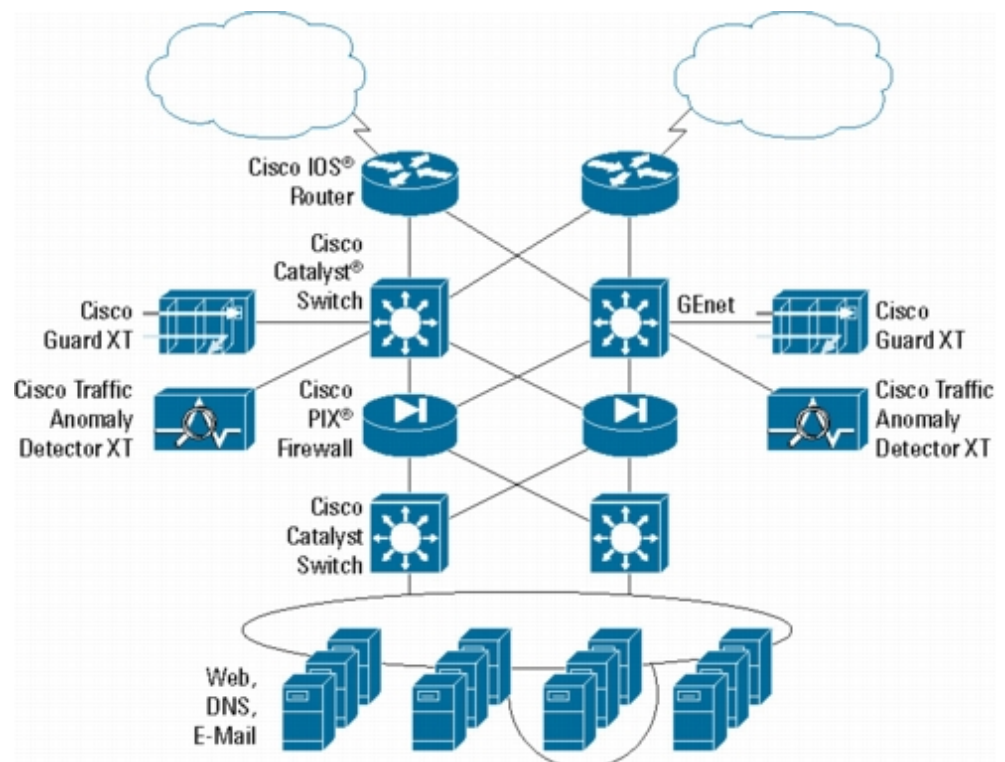
アプリケーション

Cisco Guard XT は、企業、ホスティング センター、政府機関、教育・研究機関およびサービス プロバイダー環境を DDoS 攻撃から保護する、包括的な検出および攻撃軽減対策ソリューションの一部です。Cisco Guard XT を DDoS、ワーム、その他の攻撃の存在を検出する Cisco Traffic Anomaly Detector XT と組み合わせれば、フロー単位の詳細な攻撃分析、識別、および抑制サービスを実行でき、攻撃トラフィックをブロックしてネットワーク動作の混乱を防止するために必要な情報が得られます。

Cisco Traffic Anomaly Detector XT は、攻撃の危険性を特定すると、ターゲット デバイスへ向かうトラフィックのみをルート変更して検査するように Cisco Guard XT に警告します。他のトラフィックはすべて正常に伝送されるので、業務全体への影響は抑えられ、1台の Cisco Guard XT で多数のデバイスやゾーンを保護できます。

ルート変更されたトラフィックは、Cisco Guard XT を経由します。Cisco Guard XT は、サービス プロバイダー、企業、政府機関、教育・研究機関のネットワークの入口となるアクセス ポイントから ISP のバックボーンとのピアリング ポイントに至るまで、ネットワーク内の任意の場所に設置できますが、通常はクリティカル パスから離して配置されます。このルート変更されたトラフィックに対して精密な検査が行われ、「不正な」フローと適正なトランザクションとが識別され、分離されます。これにより、攻撃パケットは識別され、除去されますが、適正なトラフィックは元の宛先へと転送されるので、正しいユーザとトランザクションは常にネットワークを通過でき、最大限のアベイラビリティが保証されます。

図 2



主な機能と利点

多段階の検証

Cisco Guard XT では、フロー単位の詳細な分析が実行され、攻撃トラフィックは極めて正確にブロックされますが、適正なトランザクションは正常に伝送されます。

この革新的なブロッキング方式は、シスコシステムズが開発した MVP アーキテクチャに基づいています。このアーキテクチャでは、インタラクティブな複数の防御レイヤが設けられていて、あらゆるタイプの攻撃を正確に識別してブロックします。ダイナミック フィルタリングおよびアクティブ検証テクノロジーが組み込まれたプロファイル ベースの高度な異常識別エンジンによって、あらゆるタイプの攻撃をすばやく自動的に防御することが可能になっており、まったく新しい未知の (Day Zero) 攻撃にも対処できます。さらに、プロトコル分析およびレート制限機能が装備されているので、有効なトラフィックのみが下流側のデバイスを圧倒しない規模で伝送されることを保証できます。

また、Cisco Guard XT に内蔵された「ゾンビ キラー」テクノロジーは数十万もの分散したゾンビ ホスト (最も一般的で阻止が困難な DDoS 攻撃の送信元) から仕掛けられる攻撃も含めて、あらゆるタイプと規模の攻撃を識別してブロックできます。

マルチギガビットのパフォーマンス

各 Cisco Guard XT には、攻撃分析およびクリーニングをサポートする専用のネットワーク プロセッサが装備されているため、スタンドアロン モードでギガビット ライン レートでの処理が可能です。これにより、脆弱化されたゾンビ ホストのような多数の分散した攻撃者から仕掛けられる攻撃も含めて、大規模な DDoS 攻撃を防御できます。

また Guard XT がサポートする独自のクラスタリング アーキテクチャは、攻撃処理レートとゾンビ防御能力の両面で、段階的な拡張を可能にしています。そのため、サービス プロバイダー、企業、政府機関、教育・研究機関のネットワーク環境でも、最も深刻な脅威からの保護に対応できます。

Cisco Guard XT は、最大限の信頼性を確保し、設置を容易にするために、ルーティング ピアとしてクリティカル パスから離して配置されます。また、ターゲットとなっているゾーンへ向かうトラフィックのみをルート変更してクリーニングするため、コスト効率の高いリソース使用と拡張が可能です。

マルチレベルのモニタリングおよびレポート機能

Guard XT には、わかりやすい Web ベースの GUI * が装備されているので、ポリシーの定義、動作のモニタリング、およびレポートの作成が簡単にできます。

モニタリングとレポート作成には複数のレベルが用意されているため、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、広範囲にわたる詳細なリアルタイム データおよび履歴データを利用できます。攻撃レポートでは、個々の攻撃の詳細情報(特性、識別されたゾンビの一覧、および使用された特定の対抗措置など)が提供されるので、セキュリティの専門家は、これらの情報に基づいて Cisco Guard XT のセキュリティ ポリシーについての検討や調整ができます。

一方、サービス プロバイダーは、顧客レベルの履歴サマリーを利用して、攻撃の多様性、期間、および規模に対する効果的な保護措置について、簡単にレポートできます。さらに、インタラクティブモードでは、推奨されるアクションとポリシーをアクティブ化する前に検討して承認するようにしたり、必要に応じて攻撃への対応を手動で制御できます。

* 英語 GUI のみの提供となります。

まとめ

サービス プロバイダー、ホスティング センター、企業、政府機関、教育・研究機関向けに設計された Cisco Guard XT は、最も悪質な攻撃に直面しても、業務の継続性を保護できます。これによって、貴重な事業資産に強固なアベイラビリティと保護を保証できるため、ユーザは競争上の優位性を得られます。

製品仕様

表 1 製品仕様

メモリ	2 GB DDRAM
ハードドライブ	80 GB
インターフェイス	ギガビット イーサネット× 2 100BASE-T × 2(管理用)
動作温度	10 ~ 35°C(50.0 ~ 95.0°F)
保管温度	10 ~ 43°C(50.0 ~ 109.4°F)
湿度	動作時: 8 ~ 80% 保管時: 8 ~ 80%
電源装置	デュアル 110 ~ 220 V, 350 W
重量	28.2 kg/62 ポンド
高さ	8.53 cm/3.36 インチ
幅	44.5 cm/17.5 インチ
奥行	69.9 cm/27.5 インチ
ラックマウント	可能

管理	セキュア Web ベース GUI(英語のみ) CLI: コンソール、Telnet、SSH Cisco (Riverhead) SNMP MIB および MIB II TACACS+ Syslog
認定規格	UL 認定 CE FCC ルール Part 15 準拠
攻撃に対する保護	<ul style="list-style-type: none"> • スプーフィングおよび非スプーフィング攻撃 <ul style="list-style-type: none"> ◦ TCP (SYN、SYN-ACK、ACK、FIN、フラグメント) ◦ UDP (ランダム ポート フラッディング、フラグメント) ◦ ICMP (到達不可能、エコー、フラグメント) ◦ DNS • クライアント攻撃 <ul style="list-style-type: none"> ◦ 非アクティブおよびすべての接続 ◦ HTTP Get フラッディング • BGP 攻撃

発注情報

表 2 発注情報

製品名	製品番号	SMARTnet® 番号
Cisco Guard XT 5650 (LC コネクタ付き 1000BASE-SX マルチモード光ファイバポート、デュアル AC 電源、RAID を装備)	AGXT-5650-MMF-A-K9	CON-SNT-AGX5650M
Cisco Traffic Anomaly Guard XT アプライアンス 5.0 ソフトウェア	SC-AGXT-5.0-K9	

シスコ製品の購入方法の詳細は、「[購入案内](#)」を参照してください。

テクニカル サポート サービス

お客様が大規模な組織であるか、営利企業であるか、またはサービス プロバイダーであるかにかかわらず、シスコは、お客様のネットワーク投資の収益を最大限に高めることを目指しています。シスコでは、各種のテクニカル サポート サービスを提供しており、ご使用のシスコ製品で動作を効率化し、高いアベイラビリティを維持し、最新のシステム ソフトウェアを活用できるように支援しています。

シスコのテクニカル サポート サービスでは、以下のような機能を提供して、ネットワーク投資の保護と、業務上重要なアプリケーションを実行しているシステムのダウンタイムの最小化を実現しています。

- シスコのネットワーク専門家がオンラインと電話でサポート
- 障害または問題が発生した場合の単なる対応策ではなく、ネットワーク運用には不可欠の一部としてソフトウェアのアップデートとアップグレードを常時提供することにより、予防的なサポート環境を実現
- シスコの技術的知識とリソースをお客様の要求に応じて提供
- お客様の技術スタッフのリソースを育成することにより、生産性を向上
- リモート テクニカル サポートに加えてオンサイトのハードウェア交換サービスを提供
- シスコのテクニカル サポート サービスには、次のものがあります。
 - Cisco SMARTnet サポート
 - Cisco SMARTnet オンサイト サポート

- シスコ ソフトウェア アプリケーション サービス (Software Application Support および Software Application Support plus Upgrades)

詳細は、次のサイトをご覧ください。<http://www.cisco.com/jp/services/>

©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

お問い合わせ先