INSUNG 인성디지탈

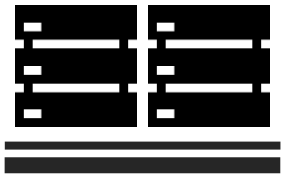
DeepFinder

Cloud Web Application Firewall

The Best Choice for Web Security and Web Application Protection!

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

ウェブファイアウォール



現在使用中のウェブファイアウォールは大部分Applianceタイプ

多くの企業がクラウドプラットホームに移転/計画中

Applianceタイプは考慮対象から除外

PROXYタイプ、クラウドウェブファイアウォールの登場

Proxy(Reverse)タイプはシステムの過負荷 / 共用ゾーンに対する負担 / DNS迂回 / 認証書の管理及びSSL Inspectionの困難 / Domain当たりの課金等によりユーザーに困難を与える。

FILTER タイプのクラウドウェブファイアウォールが代案として提示

AWS等のパブリッククラウド環境では、Appliance、Proxyタイプのウェブファイアウォールの問題点が大部分解決されたフィルタータイプのクラウドウェブファイアウォールが代案として提示

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

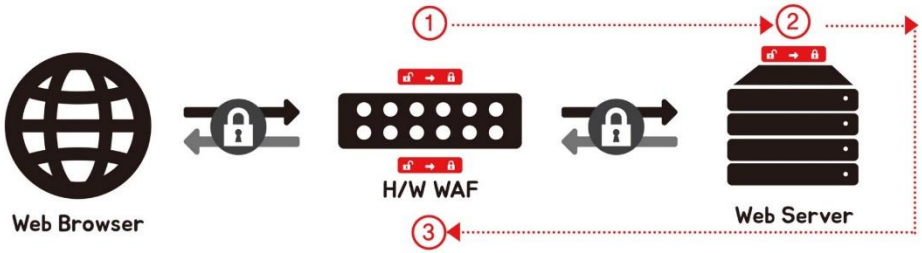
ウェブファイアウォールの比較

比較項目	Filter	Proxy, Reverse Proxy
製品名	**DeepFinder**	**P社 – W***** V, M社 – A**** SE**
構成位置	**WAS内のフィルター形態で動作**	**ELB前の段で動作、Reverse Proxyの場合はtransaction全体が企業外部網に迂回**
性能	ウェブサーバの資源使用率微々 (CPU 約 2.5% 以下、Memory 約 100M以下)	AWS検証データーなし
ウェブファイアウォール専用インスタンス構成	**別途のインスタンスが必要ない**	**別途のインスタンスが必要 (追加インスタンス費用)**
防御項目	OWASP Top 10 国情院の8大弱点 迂回攻撃の防御、内部攻撃の防御	OWASP Top 10 国情院の8大弱点
SSL処理方式	**ウェブサービスが処理 (Hooking方式)** **(Filter : 1回処理)**	**認証書の複写必要、管理困難** **(3回処理)**
SSL処理速度 **(Full Inspection)**	**速度低下なし (NIPA, TTA 検証)**	**1/5 に減少** **(約5倍遅くなる)**
重要情報流出防止	探知された重要情報の有効性検査後、流出防止	パターンによる流出防止 有効性の検査しない
政策設定方式、ログ確認 統計、報告書、パターンのアップデート	Managerを通じたウェブ形態のUI 提供	ウェブファイアウォール別のアクセス
最大Throughput	**最大限界値なし**	**装備別のThroughputがあり、これを超過時はウェブファイアウォールを交換しなければならない**
最大トラフィック超過攻撃 **(DDoSによるBPS, TPS,** **CPS 臨界値超過)**	**サーバが生きていればウェブファイアウォールも生きている**	**By-pass (ウェブファイアウォールの無力化)**
最大トラフィック超過攻撃による データー損失の可能性	なし	高い

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

ウェブファイアウォールの比較 – SSL

Proxy, Reverse Proxy ウェブファイアウォールのSSL処理過程



3回のConnectionが発生してウェブサービス速度低下

1回：Request Dataに対するハッキング検査のためのConnection

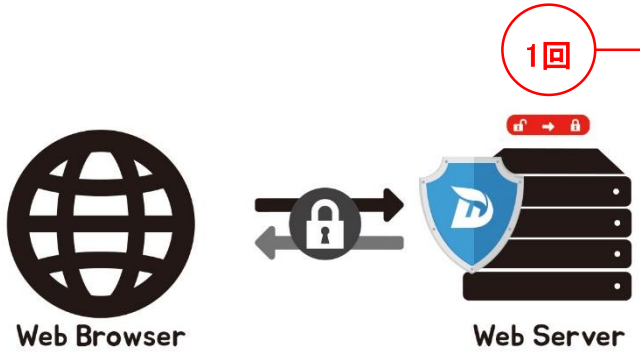
2回：ウェブサーバでプロセス処理のためのConnection

3回：Response Dataに対する検査のためのConnection

大容量のSSL処理が困難でセキュリティイシュー発生

- 大容量のSSL暗号化トラフィックが流入する場合、装備のDown、又は性能下落の発生
- SSL加速器の設置、又はSSL Inspection機能を切って置いたりする

DeepFinderのSSL処理過程



ウェブサービス速度の維持＆SSL可視性100%

ウェブサーバ内で動作するフィルタータイプのウェブファイアウォールはRequest Dataの検査、プロセスの処理、Response Dataに対する検査を一度のウェブサーバConnectionで処理します。そのため、ウェブファイアウォール機能によるウェブサービス応答速度の低下現象がありません。

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

ウェブファイアウォールの比較 – SSL

Proxy, Reverse ProxyでSSL 100% Inspection時

- SSL 検証のための追加装備が必要
- 性能維持のために加速器の導入を考慮
- システムの過負荷発生時Down 、或いはBy-passに転換
- 認証書満了時点に合わせて個別アップデートが必要

DeepFinderでSSL 100% Inspection時

- 追加装備が必要ない
- 追加リソースが必要ない
- システムの過負荷がない
- 認証書の管理が必要ない

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

クラウドウェブファイアウォール DeepFinderは

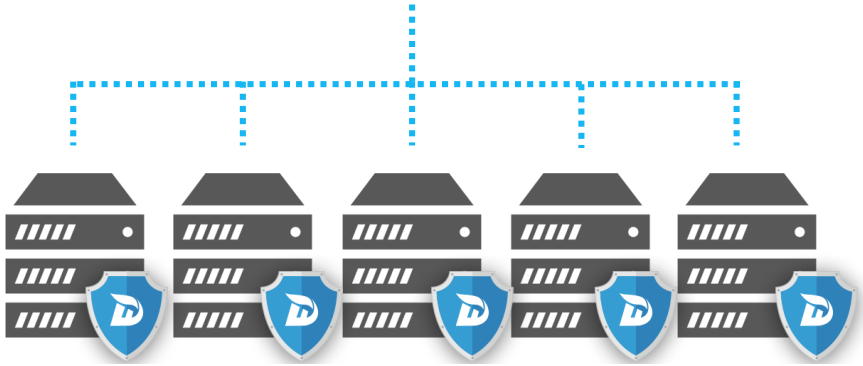
ソフトウェアフィルタータイプのウェブファイアウォールです。
大部分のクラウドプラットホームをサポートします。

利点	比較優位
1. Appliance ウェブファイアウォールの機能は基本遂行 2. 性能低下のない SSL 100% Inspection 3. ウェブファイアウォールの容量増設、License 更新の必要なし 4. ウェブファイアウォールを運用するための別途 Instance 必要なし 5. 遠隔で設置、削除、修正、政策変更可能 6. 処理容量の最大Throughputなし	1. システム変更、追加のない SSL 100% Inspection 2. 認証書の更新及び管理の必要なし 3. 最大トラフィックの限界がないので、By-pass モードに切り替わらない 4. 製品の老朽化がないので、製品のアップグレード、交換が必要ない

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

クラウドウェブファイアウォールDeepFinder

DeepFinder Manager



DeepFinder Agent In Seoul
DeepFinder Agent In Thailand
DeepFinder Agent In Busan
DeepFinder Agent In Japan
DeepFinder Agent In China

フィルタータイプ

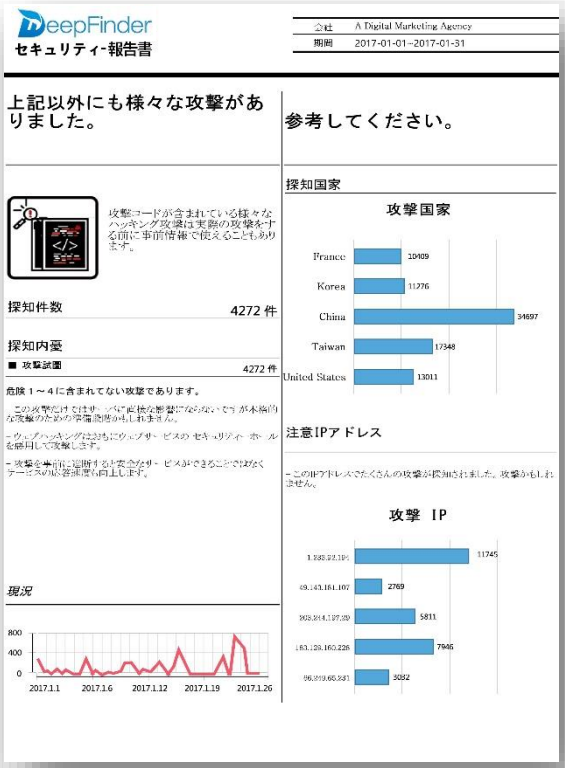
個別ウェブサーバにモジュール形態でインストールされて動作

- **クラウドに最適化されたウェブファイアウォール**
- **Managerでリアルタイム統合管理**
  - Managerで遠隔 Trouble shooting
  - 海外及び地方事業場のウェブサーバ統合管理
  - 労力・費用投入の最少化
- **SSL 可視性 100%**
  - 要請/応答トラフィックをウェブサービスの処理過程中に介入して一度に処理(Hooking)
- **S/W フィルター方式**
  - 内部網の防御
  - 既存ネットワークの変動なく構築可能
  - Hypervisor、VMに関係なくインストール
  - 様々な異機種環境のサポート
- **政策適用:リアルタイム(15秒)**

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

DeepFinderの主な特徴

C – levelのための
主な威嚇要素別セキュリティレポート



[DeepFinder ウェブ攻撃分析 – 顧客用レポート]

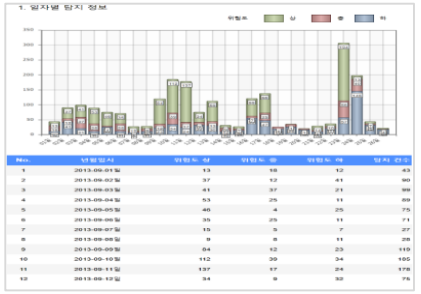
Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

DeepFinderの主な特徴

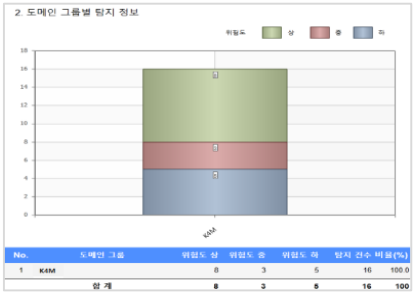
リアルタイム探知ログを基に多次元分析

類型別の詳しい分析レポート / 単位統計照会

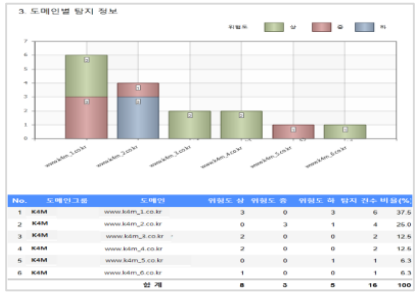
日別攻撃分析



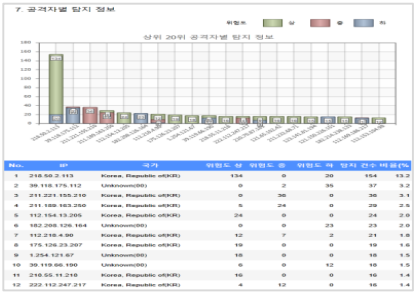
ドメイングループ別分析



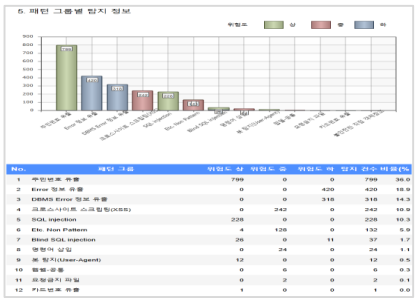
ドメイン別分析



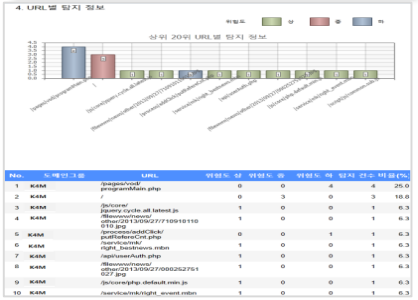
攻撃者別の攻撃分析



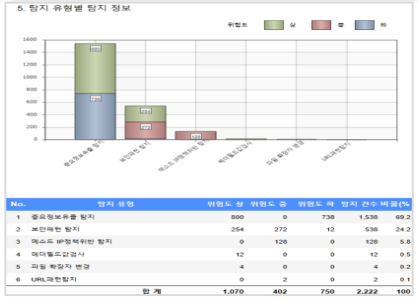
パターングループ別の攻撃分析



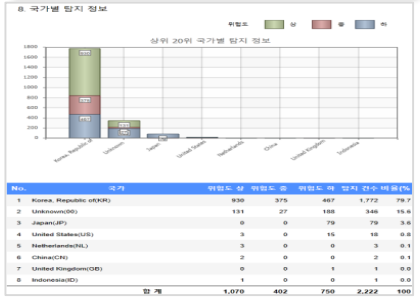
URL別の攻撃分析



探知類型別の攻撃分析



国家別の攻撃分析



[DeepFinder ウェブ攻撃分析 – 管制用レポート]

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.

감사합니다

Copyright(c) 2017 Insung Digital Co.,Ltd. All rights reserved.