

August, 2017



BIG-IP: IP Intelligence

PRESENTED BY:

F5ネットワークスジャパン

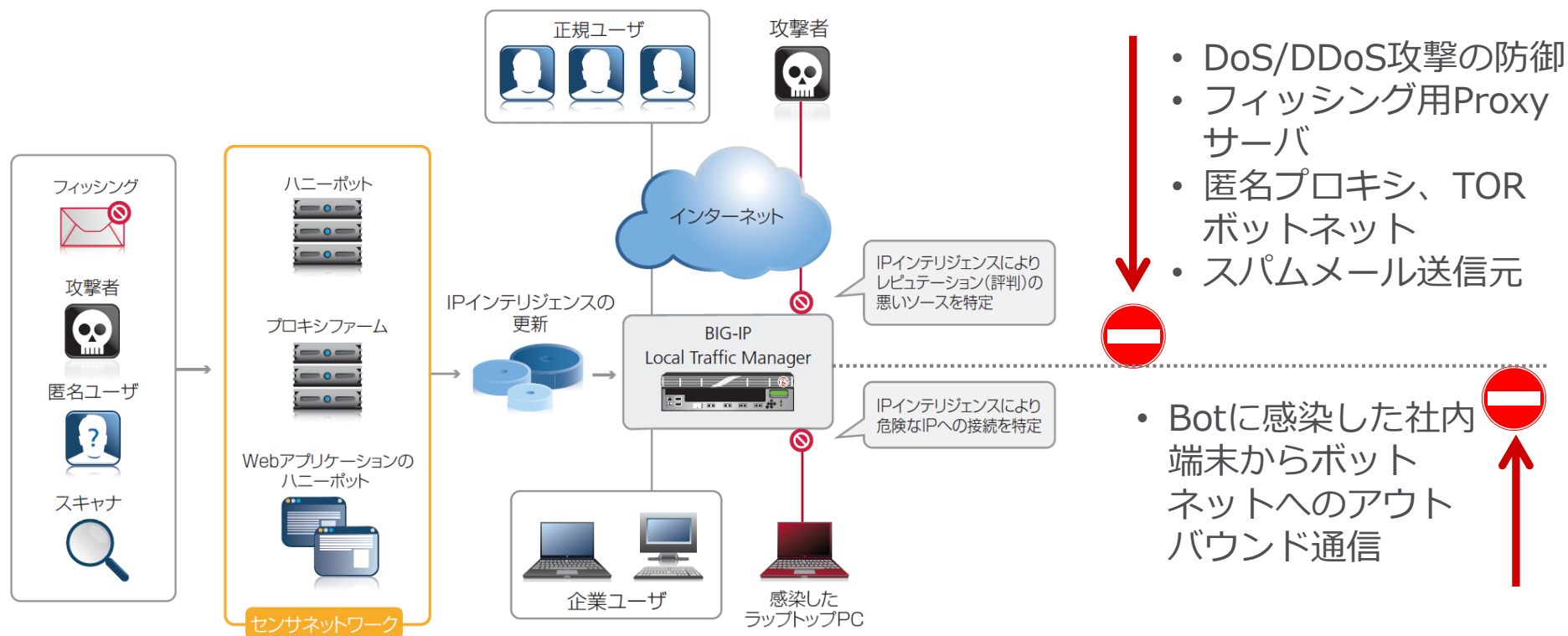
WE MAKE APPS  FASTER.
SMARTER.
SAFER.

IPインテリジェンスとは

(v11.2以降でサポート)

BIG-IPの機能モジュール

悪質なIPアドレスのデータベースを用い、ダイナミックなペリメータ（境界）セキュリティを実現



IPインテリジェンス 機能

- **IPインテリジェンス・データベースを5分間隔で更新（変更可能）**
- **IPアドレス毎に脅威を判定。次ページの8カテゴリにおいて判別される**
- **利用方法**
- 悪質なIPアドレスと判断された場合はブロックまたはアラームを上げる（BIG-IP ASMにて）
- iRulesを用いることでサーバ負荷分散等、その他のBIG-IPの機能と連携することも可能

脅威のカテゴリ

1	エクスプロイト	マルウェア、シェルコード、ルートキット、ワームやウイルスを配布するIP群
2	Web攻撃	クロスサイトスクリプティング、IFRAMEインジェクション、SQLインジェクション、クロスドメインインジェクション、ブルートフォース攻撃を含む
3	ボットネット	ボットネット、C&C、ボットマスターによって制御され、感染したゾンビマシンなど
4	スキャナ	ホストスキャン、ドメインスキャンおよび辞書ツールを使用したブルートフォース攻撃など
5	DDOS	DOS、DDOS、SYNフラッドなど
6	Reputation	レピュテーションスコアの平均値が低いIPや既知のマルウェアに感染することを確認しているIP群
7	フィッシング	フィッシングサイト、広告クリック詐欺など
8	匿名プロキシ	匿名化に用いられているプロキシ（TOR Anonymizer 含む）

ASMでの利用イメージ

- アラーム、ブロッキングなどの設定をASMから簡単に設定
- 特定のIPアドレスをホワイトリストとして記載し管理
- X-Forwarded-Forヘッダの参照もできるので、CDNを用いているWebサイト（Original Web Server）でも利用可能

The IP intelligence service provides categorization of known to be bad IPs. With this service the ASM enhance: being able to block known bad sources like phishing proxies that are used for phishing attacks , users who anonymize themselves by using anonymous proxies or the TOR network, Botnets and other sources of malicious traffic.

Block the following categories

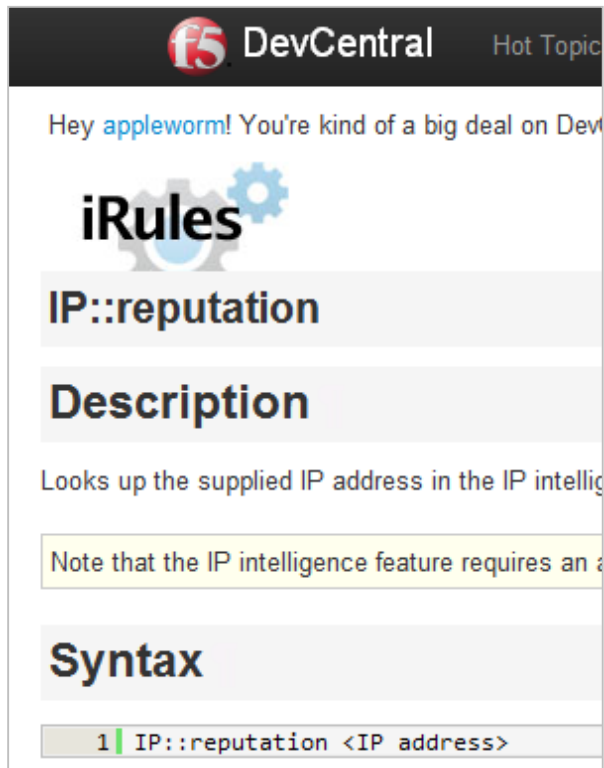
Proxy	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
Phishing	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
BotNets	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
Denial of Service	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
Scanners	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
Web Attacks	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
Reputation	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block
Windows Exploits	<input type="checkbox"/> Alarm	<input type="checkbox"/> Block

IP Intelligence Configuration

Whitelist IP Addresses	IP Address:	<input type="text"/>	Add
	Subnet Mask:	<input type="text"/>	
<div></div>			
Remove			
Ignore for policy building	<input checked="" type="checkbox"/> Enabled		
Note: Enabling this setting will cause the automatic policy builder and manager to ignore any recommendation originated from a blacklisted source IP.			

Save

iRuleからの利用イメージ



BIG-IP LTM, DNS等、ASM以外のモジュールからでも利用可能。

IP::reputation コマンド詳細は下記URLをご参照ください

<https://devcentral.f5.com/wiki/iRules.IP-reputation.ashx>

