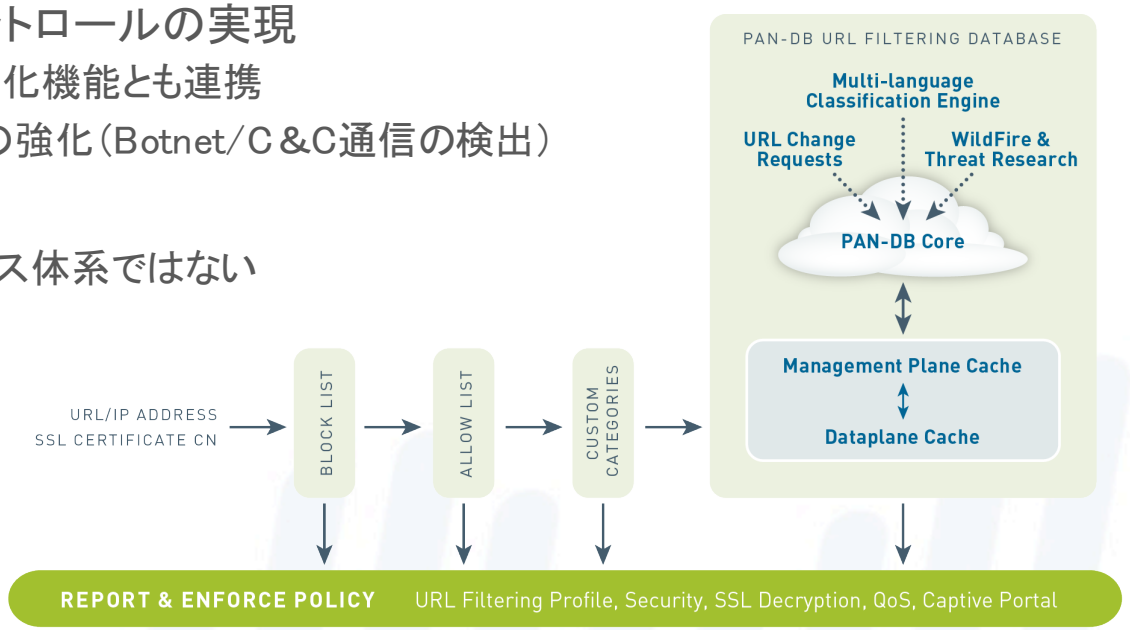
PAシリーズ URLフィルタリング
PAN-DB

paloalto NETWORKS
the network security company™

PAN-DB URLフィルタリング機能の概要

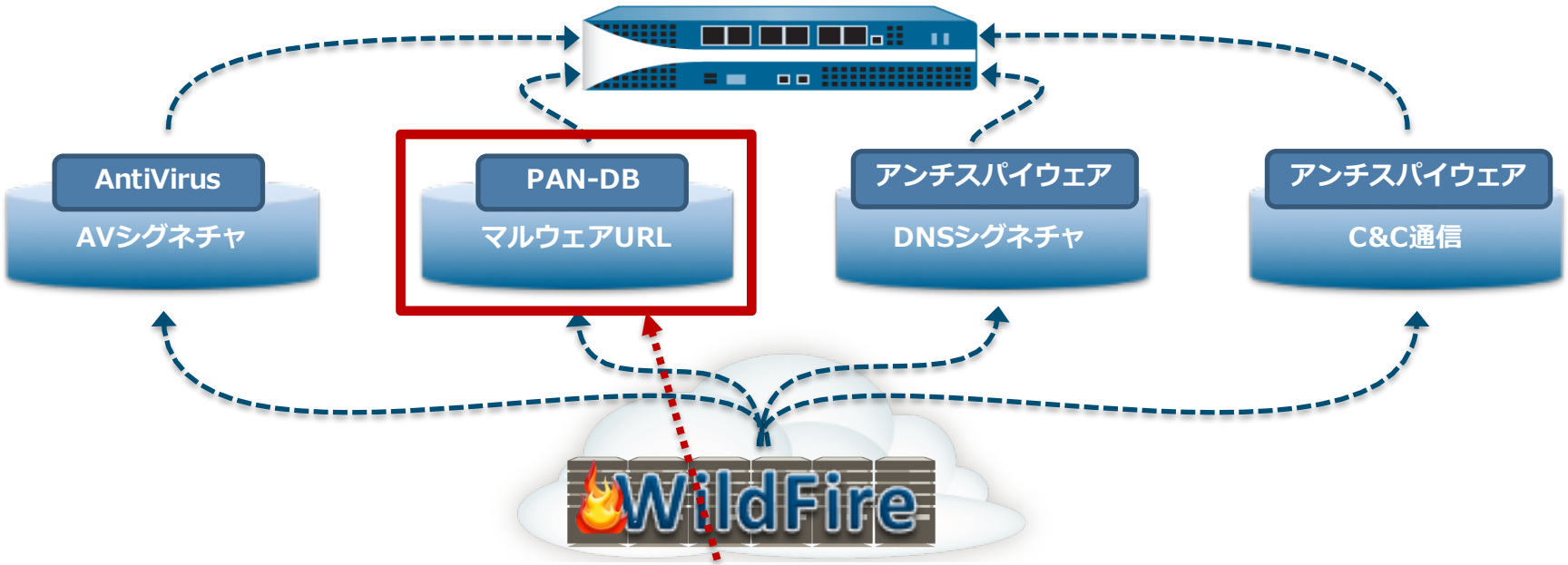
- PAシリーズ次世代ファイアウォールに組み込まれたURLフィルタリング機能
  - 61カテゴリおよびカスタムカテゴリによるきめ細やかなURLアクセス制御
  - 日本を含む9言語のURLデータベースが利用可能
- 主な特長
  - 高速な処理の実現
    - クラウドとの連携により常時最新情報とSync
    - メモリキャッシュによる高速な処理を実現
  - きめ細やかで高度なアクセスコントロールの実現
    - アプリケーション制御やSSL復号化機能とも連携
    - 標的型攻撃に対する出口対策の強化（Botnet/C&C通信の検出）
  - 低コスト
    - クライアント台数単位のライセンス体系ではない
  - シンプルな運用管理
    - FWとProxy(URLフィルタ)を個別に管理する必要がないためTCO削減が可能に



PAN-DB：標的型サイバー攻撃対策における優位性

- マルウェアサイト等のハイリスクなサイトの情報が充実したデータベース
- 従来のURLフィルタ製品には出来ない、Web以外の通信も含めたさまざまな内部ログの相関分析により、未知のマルウェア感染端末の発見やC&C通信の検知が高精度で可能に

PAN-DB：WildFireとの連携による優位性



Wildfireで解析した、マルウェアが実際に通信を行う情報をDBにフィードバック

BEHAVIORAL SUMMARY

This sample was found to be **malware** on this virtual machine.

Behavior
Created a file in the Windows folder
Created an executable file in a user folder
Created or modified a file
Started a process
Created an executable file in the Windows folder
Modified the Windows Registry
Modified the Windows Registry to enable auto-start
Modified Internet Explorer security settings
Used a short HTTP header
Used the HTTP POST method
Connected directly to an IP address over HTTP

HTTP REQUESTS

HTTP Method	URL	User-Agent
GET	sh[redacted]ontent/uploads/2014/03/tip_of_the_day_home.jpg	
POST	14[redacted]47.77/callback/bo.php	
GET	evcs[redacted]tec.com/evcs.crl	Microsoft-CryptoAPI/5.131.2600.5512
POST	14[redacted]77/callback/bo.php	
POST	1[redacted]77/callback/bo.php	
GET	d[redacted]om/pca3-g5.crl	Microsoft-CryptoAPI/5.131.2600.5512
POST	14[redacted]77/callback/bo.php	
GET	cs[redacted]n.com/CSC3-2010.crl	Microsoft-CryptoAPI/5.131.2600.5512

WILDFIRE

paloalto NETWORKS

paloalto NETWORKS

PAN-DB：その他高度なアクセスコントロールも実現

- SSL複合化機能（SSL Decryption）
  - SSL通信に対する複合化処理の有無をWebカテゴリ単位で指定可能
    - 利用例1：金融系Webサイトへのアクセス時はSSL複合化検査を行わない
    - 利用例2：Unknown(未知)のWebサイトアクセス時、SSL複合化を行い脅威のスキャンを実行

	Source			Destination					
Name	Zone	Address	User	Zone	Address	URL Category	Action	Type	Decryption Profile
Decrypt Mail Only	any	any	any	any	any	web-based-email	decrypt	ssl-forward-proxy	deny-decrypt-failures

- QoS機能
  - Webカテゴリ単位でQoSによる優先制御を行う事が可能
    - 利用例：業務時間内はストリーミングメディアサイトに対する通信の優先度を下げる

	Source			Destination				
Name	Zone	Address	User	Zone	Address	Application	URL Category	Schedule
Limit streaming media	any	any	any	any	any	any	streaming-media	Work Days

ユーザのプライバシーに配慮したセキュリティ検査や、業務に悪影響を
及ぼす可能性があるWeb通信に対する能動的なコントロールを実現
※URLフィルタリング製品単体、複数製品の組み合わせによる実現は容易ではない

PAシリーズ　URLフィルタ機能の利用メリットまとめ

PAN-DB	従来のURLフィルタ製品
カテゴリベースのアクセス制御	○
サンドボックス解析情報のデータベースフィード	×
SSL復号化対象のカテゴリベース制御	×
QoS対象のカテゴリベース制御	×


paloalto
NETWORKS
the network security company™