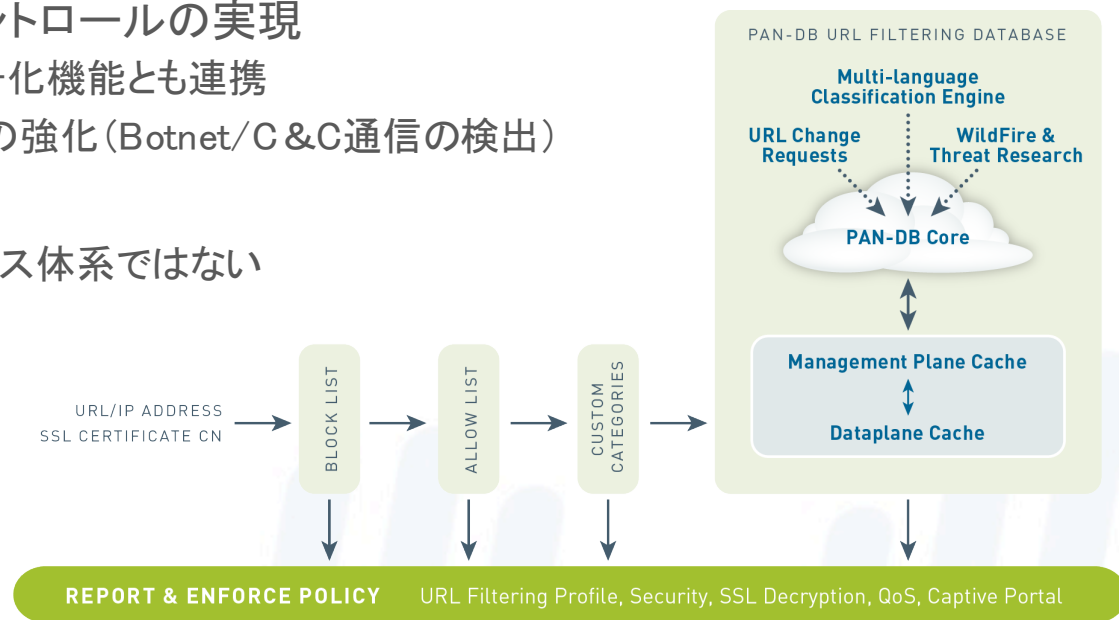


PAシリーズ URLフィルタリング PAN-DB

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

振る舞いベースのボットネットレポート機能

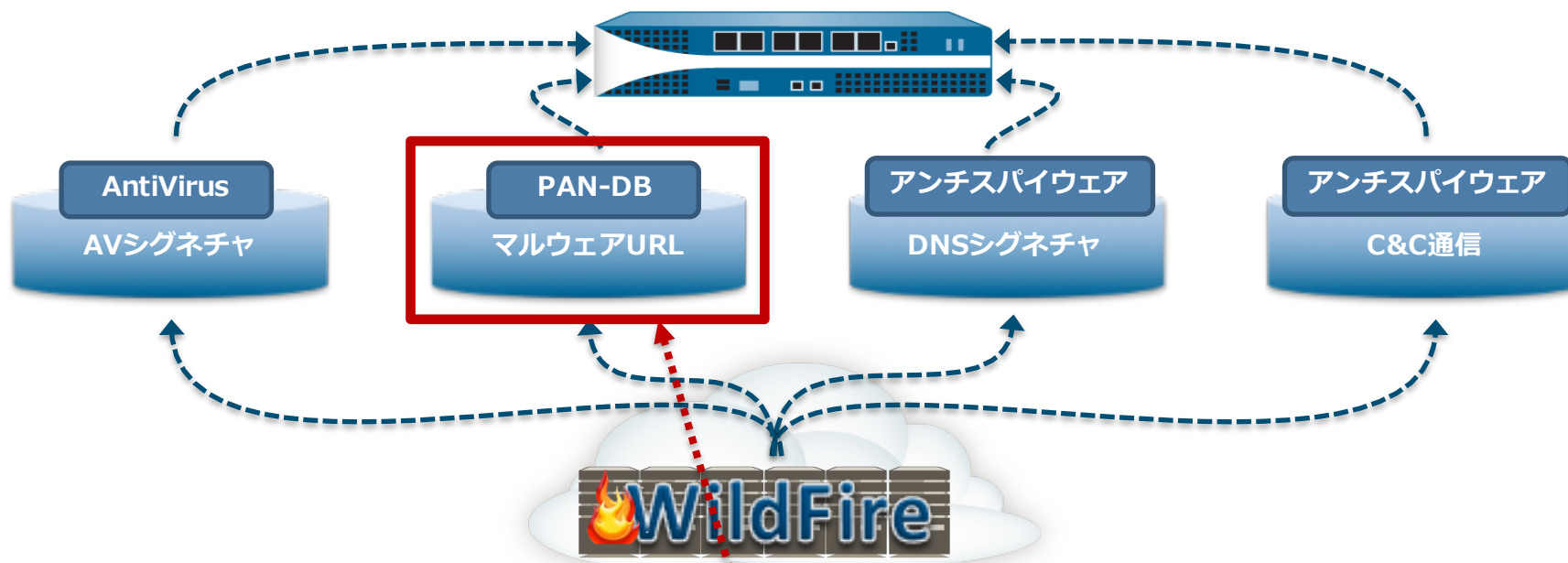
The screenshot displays a table of botnet reports with the following columns: Confidence, IP Address, and Description. The table lists various activities such as downloading executables from malicious URLs, repeatedly visiting the same URLs, and IRC traffic. Callouts provide detailed information about specific entries, such as the number of downloads and visits to a particular URL.

Confidence	IP Address	Description
5	134.154.168...	Downloads executable(s) from malicious URL ics.dickpotato.tv/software/dickpotatoliteclient
4	134.154.171...	Repeatedly (8) visits the same malicious URL interstitial.powered-by.securewebsiteaccess.com/fd2fed27b5ce840
3	134.154.170.53	Repeatedly (22) downloads executables from the same unknown URL 15.1.0.101/malware01.exe . Repeatedly visited (46) the same URL 168.143.169.168/twirl/images/word_area_sm.png
2	134.154.233...	IRC traffic
4	134.154.170...	IRC traffic
2	82.146.58.53	Repeatedly (6) visits the same URL 78.24.220.98
2	134.154.169.46	Repeatedly (20) visits the same URL 212.227.96.110/rpc.html?e=
2	134.154.168.14	Repeatedly (28) visits the same URL 218.93.210.82/api/tj/idonline_7001.txt
2	134.154.168.24	Repeatedly (24) visits the same URL 134.154.209.238/Images/Site/CSUEastBay/csueb_wordmark.gif
2	64.62.252.25	Repeatedly (6) visits the same URL 134.154.209.238/Images/Site/CSUEastBay/csueb_wordmark.gif
2	134.154.175.33	Repeatedly (56) visits the same URL 134.154.209.238/Images/Site/CSUEastBay/csueb_wordmark.gif
2	62.109.0.34	Repeatedly (7) visits the same URL 78.24.220.98/
2	98.119.244.133	Repeatedly (5) visits the same URL 134.154.209.238/Images/Site/CSUEastBay/csueb_wordmark.gif
2	134.154.171.81	Repeatedly (5) visits the same URL 112.90.136.41/GetFile
2	134.154.168.18	Repeatedly (6) visits the same URL 121.14.102.15/
2	134.154.171...	Repeatedly (6) visits the same URL 119.145.146.203/6a992d55.html?staticDataType=4&uid=8337617&sid=124491949&mediaProxyIp=232524153&lossPacketNu...
2	134.154.174...	Repeatedly (14) visits the same URL 87.106.13.61/rpc.html?e=bl
2	134.154.170...	Repeatedly (6) visits the same URL 61.135.188.234/web_ime/pynet.php?durtot=546&durcon=218&durtran=234&h=7f607df8e0b25ae060b019364187e4ab&v=5.1...
2	134.154.177...	Repeatedly (9) visits the same URL 67.244.96.75/
2	60.249.232.226	Repeatedly (8) visits the same URL 134.154.183.25/
2	134.154.169.61	Repeatedly (40) visits the same URL 82.165.142.210/rpc.html?e=bl
2	67.202.56.76	Repeatedly (48) visits the same URL 134.154.30.10/robots.txt
2	134.154.177...	Repeatedly (7) visits the same URL 75.126.220.20/

Callouts from the image:

- Repeatedly (22) downloads executables from the same unknown URL 15.1.0.101/malware01.exe . Repeatedly visited (46) the same URL 168.143.169.168/twirl/images/word_area_sm.png
- 未知カテゴリの同じURLから実行ファイルを22回ダウンロード
- 同じURLに46回アクセス
- Repeatedly visited (96) the same malicious URL serw.myroittracking.com/newServing/tracking_id.php?d=ads.lzjl.com&r=http://ads.lzjl.com/newServing/tracking_id.php?b=1&
- マルウェアカテゴリの同じURLに96回のアクセス

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]content/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	[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



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

Name	Source			Destination		URL Category	Action	Type	Decryption Profile
	Zone	Address	User	Zone	Address				
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

Name	Source			Destination		Application	URL Category	Schedule
	Zone	Address	User	Zone	Address			
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™