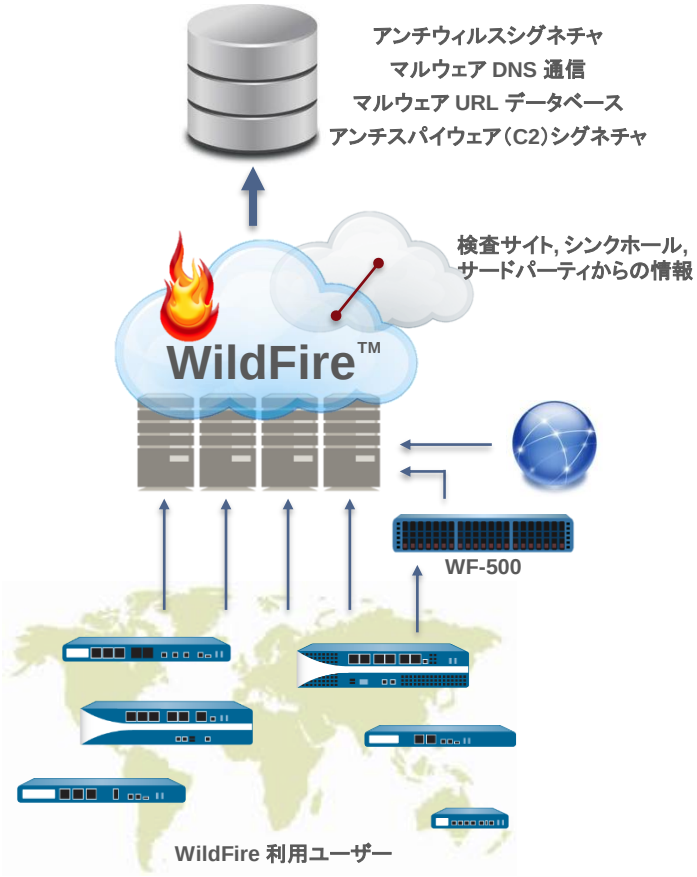
WF-500のご紹介

パロアルトネットワークス株式会社

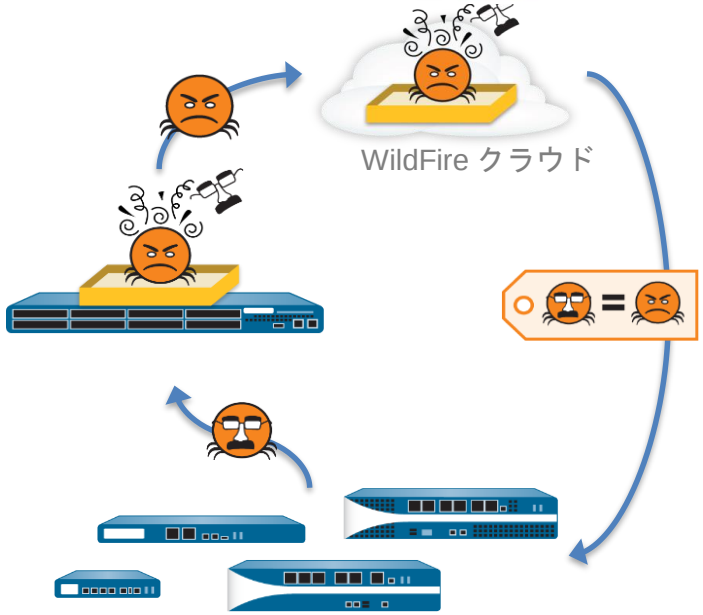
サンドボックスサービス：WildFire



- **スケーラビリティ** が高いクラウドベースのアプローチによって幅広い環境からの”未知”通信を分析
- 高度に **カスタマイズ** された“サンドボックス”によりファイルを分析
- 最新の脅威に対応できるよう常に分析や検知ロジックを **更新**
- PDF, Office, Java, Android APKといった新しいファイルタイプやOSバージョンにも **拡張**

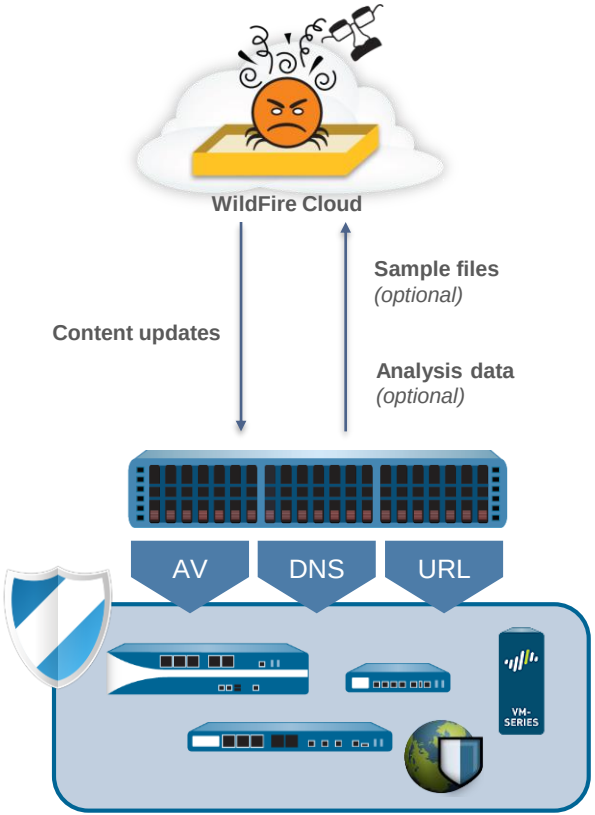
WildFireアプライアンス　WF-500

- オンプレミス導入用のWildFireアプライアンス
- PA シリーズがセンサーとしてファイルを送信
- ファイルの解析は WF-500 上で行う
- マルウェア判定となったファイルだけをクラウドに送信することも設定により選択可能
- サンドボックスからのインターネット接続に対応（設定により選択可能）
- シグネチャ配信の仕組みはこれまでと同一



WF-500機能拡張（6.1以降）

- WF-500上でローカルシグネチャ生成をサポート
  - WFクラウドに検体を送付することなく、シグネチャ生成可能
- 以下の形態のローカルシグネチャをサポート
  - アンチウイルスシグネチャ（検体をブロック)
  - DNSシグネチャ(C&C通信をブロック)
  - PAN-DBのマルウェアカテゴリーにURLをフィードバック
- ローカルシグネチャは、管理するファイアウォール(全モデル)に配信可能
- ローカルシグネチャは、5分おきに更新
- オプション設定でWildFireクラウドに検体、Analysisレポートをシェア可能
- デイリーのシグネチャ更新をWF-500でダウンロード可能(ローカルシグネチャの生成機能に必要)
- WF-500でWildFire APIをサポート
- WF-500上の仮想端末としてWindows7(64bit)をサポート



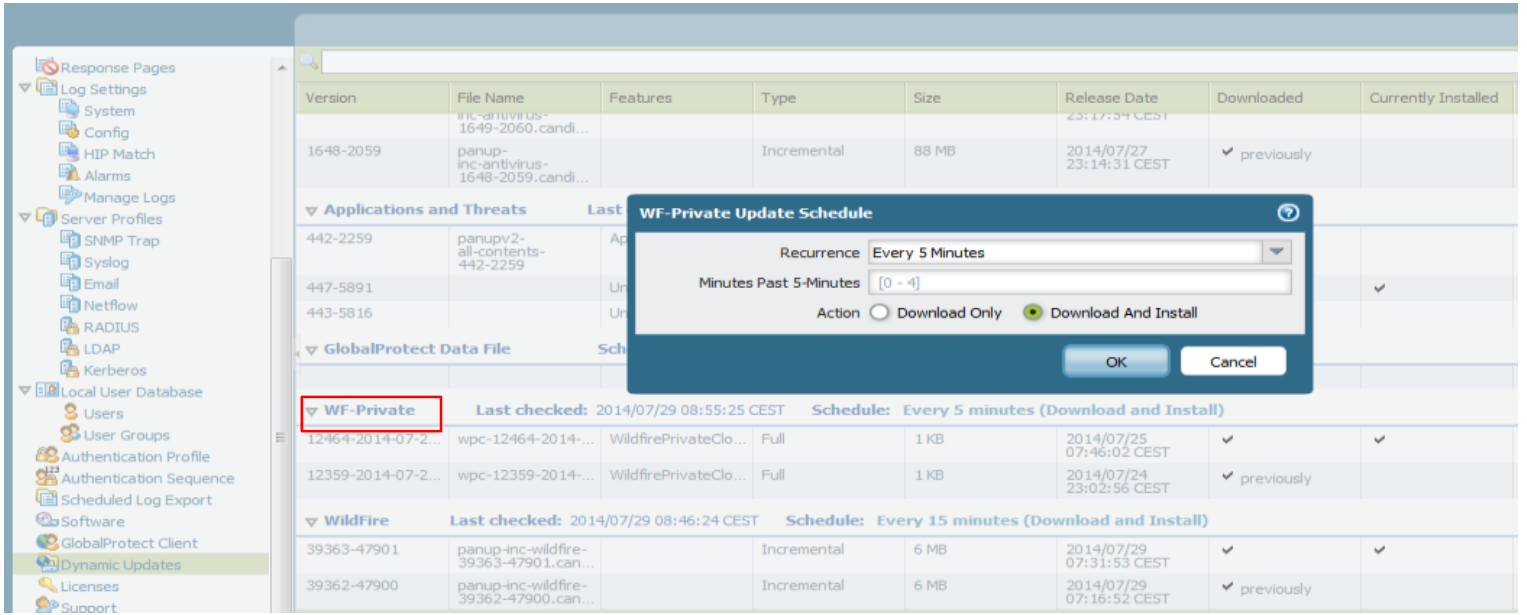
WF-500　ローカルシグネチャ注意事項

- ローカルシグネチャ(AV, DNS, マルウェアURL)は、それぞれ最大10,000シグネチャ/最大6か月まで保持可能
- 上記の上限値に達した場合、古いシグネチャから順に削除される。ただし、検体が既存のローカルシグネチャにヒットした場合は、このシグネチャはローカルシグネチャリストの順番の最新ものとして順位づけられる
- ファイアウォールは、ローカルシグネチャ(AV, DNS, マルウェアURL)を5分毎にダウンロード可能
- ローカルシグネチャ生成で使用した検体、分析結果レポートをWildFireクラウドにシェアする場合、5分毎にシェアされる
- ローカルシグネチャをファイアウォールで使用しても、従来のシグネチャと同等のパフォーマンス
- WF-500で生成されたローカルシグネチャは、ファイアウォールが直接WF-500からダウンロードする
  Panorama経由でのローカルシグネチャのダウンロードは、未サポート
- Panorama上でもWF-500からローカルシグネチャのダウンロードは可能だが、ポリシーで使用する用途に限定
  (PanoramaからファイアウォールへのWF-500のローカルシグネチャの配信はできない)

ローカルシグネチャ　PA　設定例

PAのWebUIで、Deviceタブ > Dynamic Updates > WF-PrivateのSchedule設定から更新間隔を設定

(WF-500へのregistrationが行われると、WF-Privateの項目が表示される)



ローカルシグネチャ　WF-500　設定例

CLIから以下のコマンドで、ローカルシグネチャの生成のON/OFF、検体、分析レポートのWildFireクラウドへのシェアのON/OFFを設定する

```
set deviceconfig setting wildfire signature-generation ...
```

- av <yes|no> (defaultは、ON)
- dns <yes|no> (defaultは、ON)
- url <yes|no> (defaultは、ON)

```
set deviceconfig setting wildfire cloud-intelligence ...
```

- submit-sample <yes|no> (defaultは、OFF)
- submit-report <yes|no> (defaultは、OFF)

製品の位置づけ

一般的なエンタープライズのお客様

- ファイアウォールとして PA シリーズを利用
- 標的型攻撃対策にも興味がある
- 通常のアンチウィルスやアンチスパイウェア以外にゼロディマルウェアもブロックしたい
- 念のため、ネットワーク上のマルウェアをモニタリングしておきたい
- 運用の手間をできるだけ掛けたくない

WILDFIRE

パブリッククラウド

プライベートクラウドを希望するお客様

- ファイルを社外に送信できない
- 予算に限度は設けず、出来る限りのセキュリティ対策を打ちたい
- サンドボックスの運用を自社で行いたい
- 既に他社サンドボックス製品を利用していてそれを置き換えたい

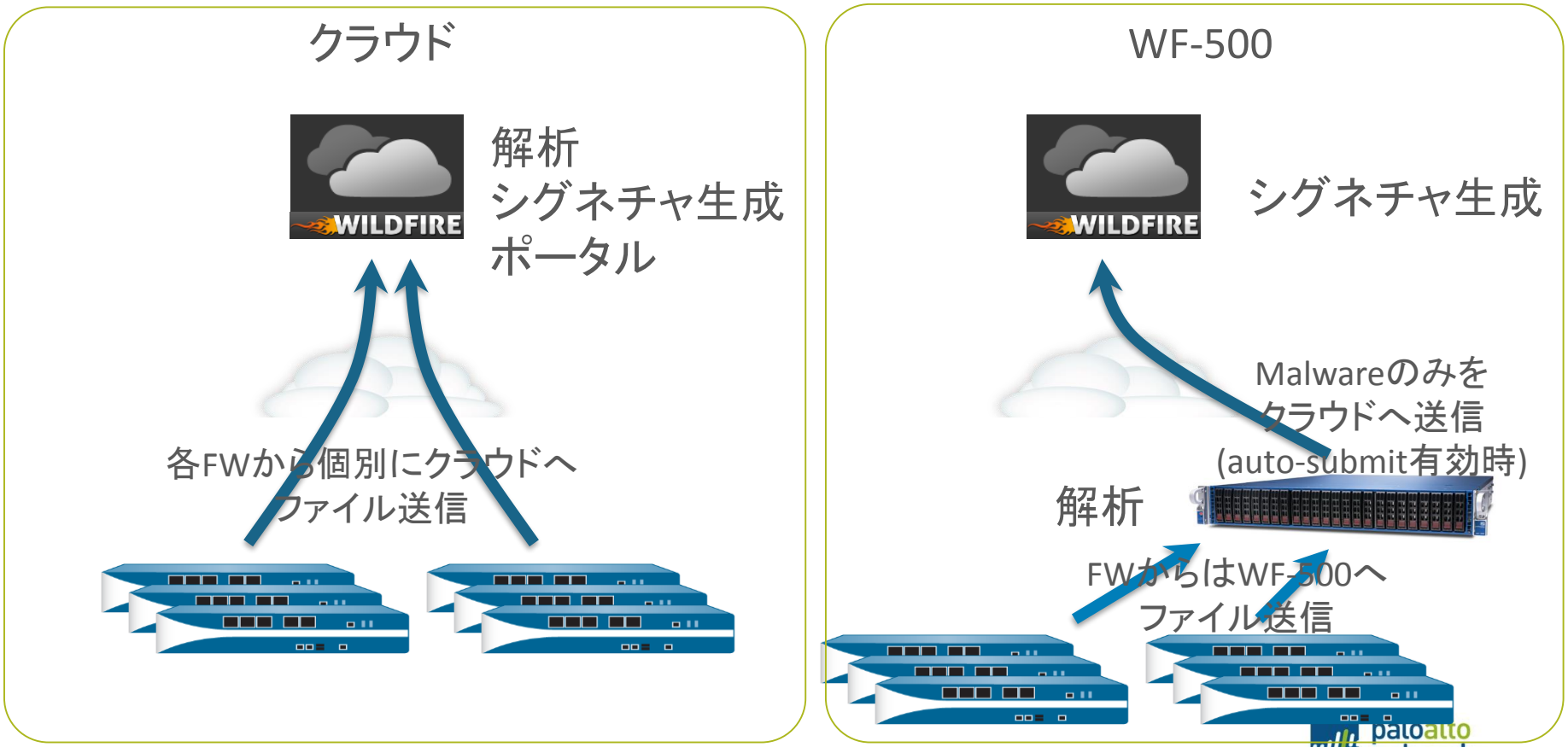
WF-500 アプライアンス

paloalto networks.

WF-500とWildFire Cloudの比較表(ver 7.0)

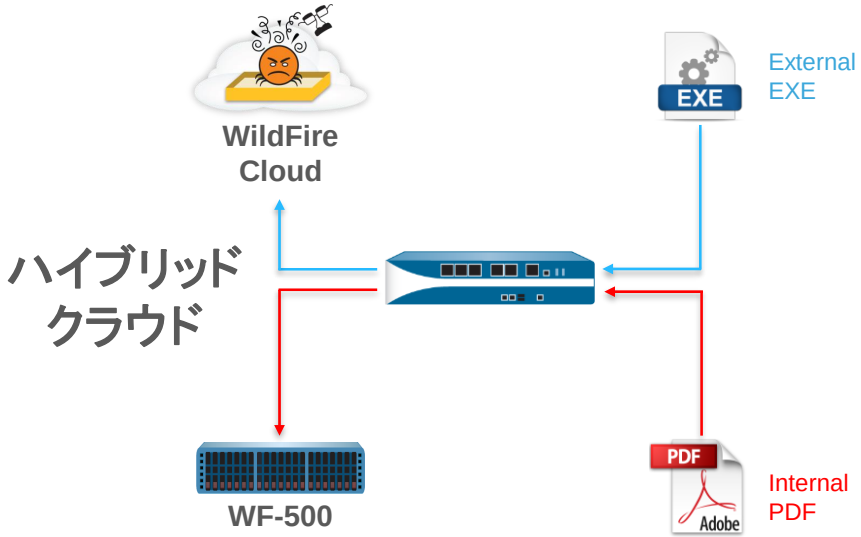
項目	WF-500	WildFire Cloud
対応ファイル	PE, Java, Office, Adobe Flash.PDF	PE, Java, Office, Adobe Flash,PDF, Android APK
クラウドの利用	設定により選択可	常に利用
解析用VMの種類	1 (5種類から選択)	Windows XP 32 bit Windows 7 64bit, Android OS 2.3, 4.1
処理能力	10,000 / 日（動的解析）	無制限
電子メールリンク分析	✔ （Ver 7.0より対応）	✔
マルチバージョン解析	未対応	✔
API	✔ （Ver 6.1より対応）	✔

構成イメージ

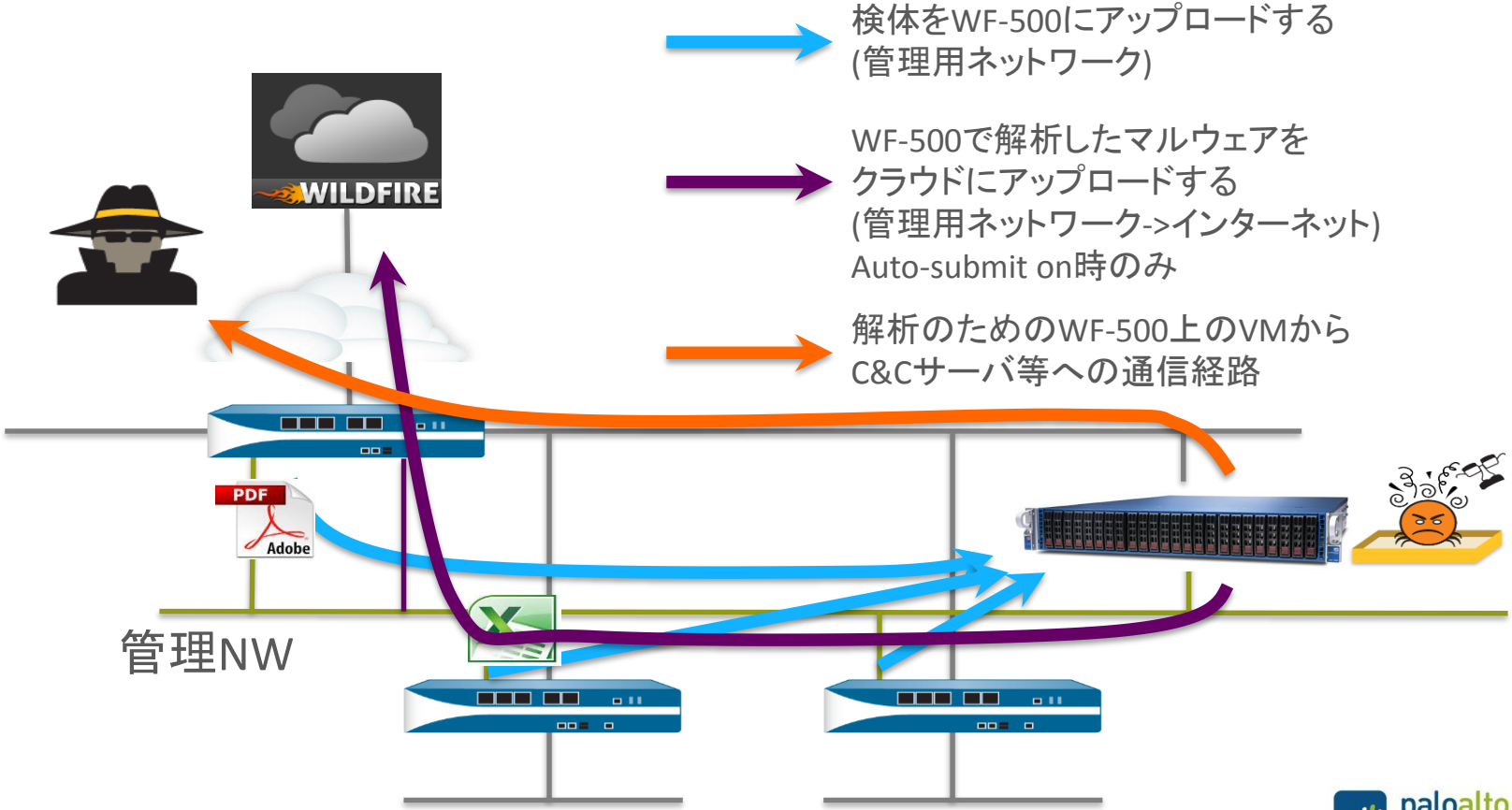


構成イメージ（ハイブリッドクラウド）

- ハイブリッドクラウド
  主な効果
  - WildFireクラウドまたはWF-500への解析をポリシーベースで緻密にコントロール
    例）外部からのPEファイルはクラウドにて検査、内部でやり取りされるファイルはWF-500で検査といった形でWildFireの解析をPAシリーズのポリシーで柔軟に制御可能
    （PAシリーズ Ver 7.0以降で対応）

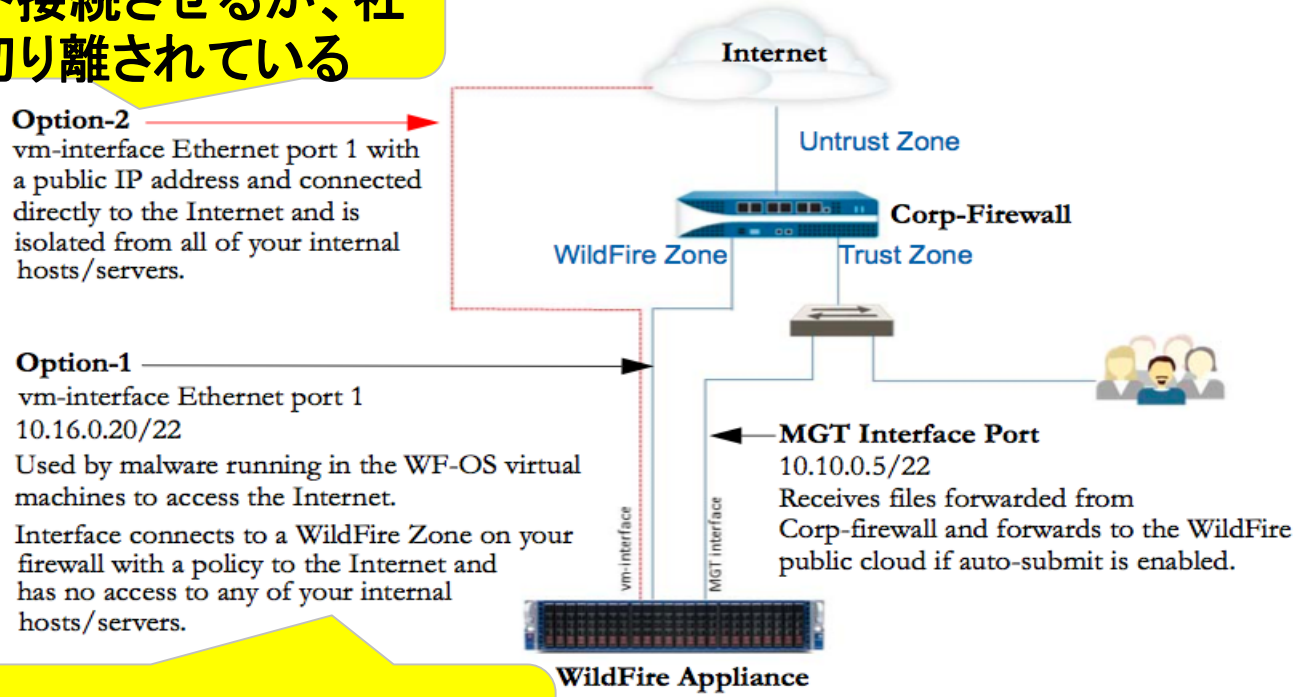


WF-500のネットワーク構成



WF-500のネットワーク構成

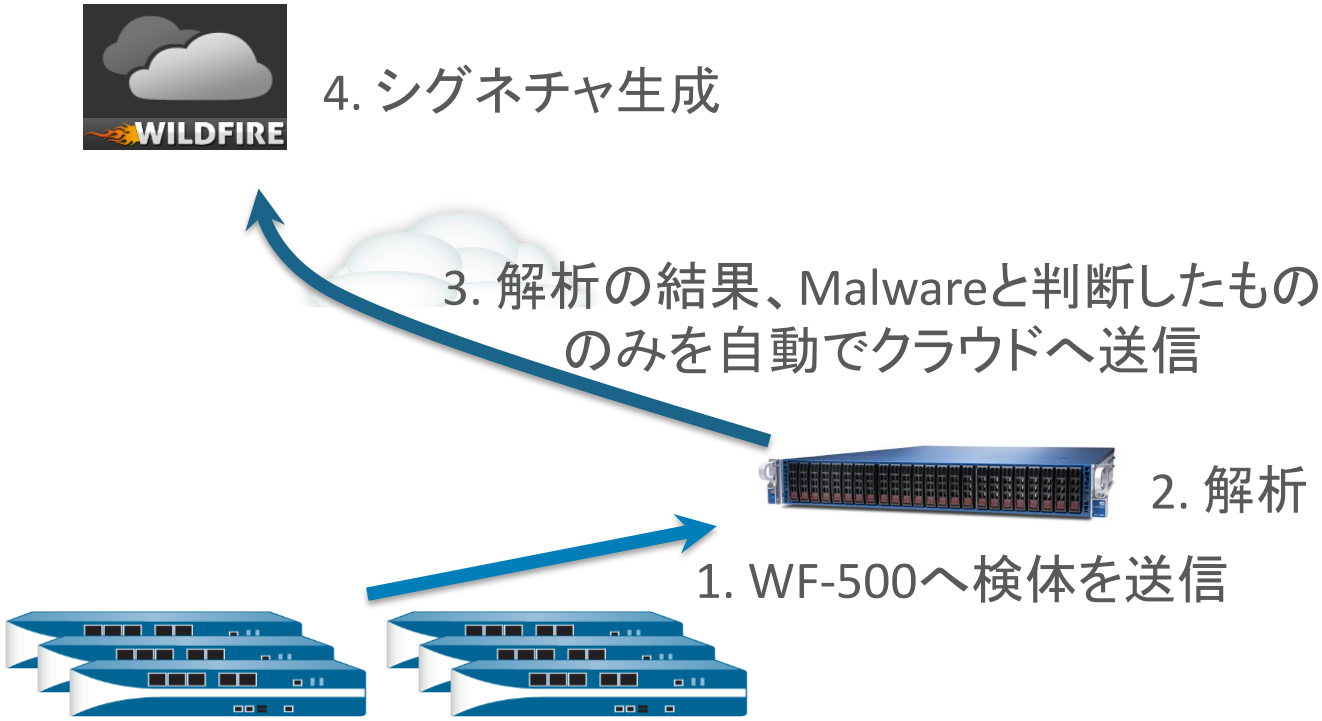
オプション2
直接インターネット接続させるが、社内ネットワークと切り離されている



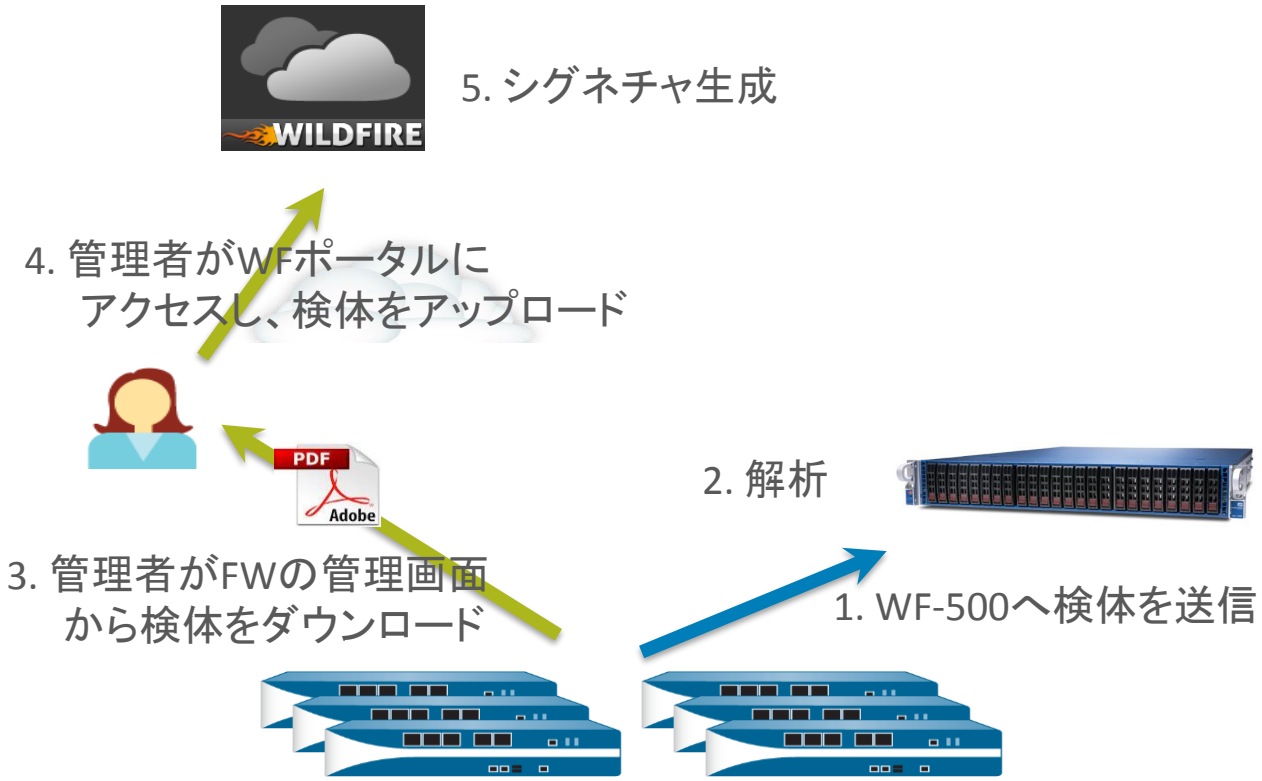
オプション1
WildFireOSの仮想マシンで検出されたマルウェアがインターネットアクセスを行う

paloalto networks.

auto-submit on時の動作



auto-submit off時の動作



paloalto networks®

the enterprise security company™