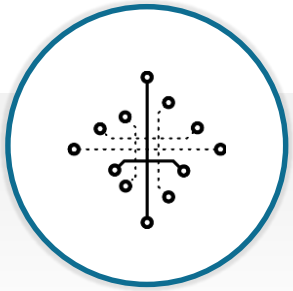
最新機能Update！
最新版OS PAN-OS 9.0のご紹介と Auto Tagによる自動制御

May 2019

パロアルトネットワークス株式会社

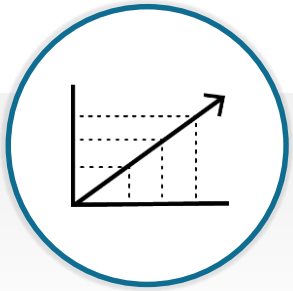
PAN-OS 9.0: 統合化された革新的な新機能により攻撃を防止

統合DNSセキュリティ
DNSを悪用する攻撃を
高度に無力化



あたらしいポリシー最適化機能
リスクのある危険なセキュリティ
ポリシーのギャップを解消

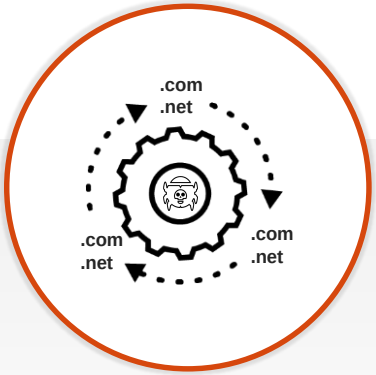
PA-7000 シリーズ
業界最速の性能を誇る
次世代ファイアウォール



60を超える新機能 により、時間の節約と強力なサイバー攻撃の防御を実現

統合化された
DNSセキュリティ

セキュリティ検査をすり抜けるDNSを悪用した攻撃



限定的な検査

DNSはコマンド＆コントロール(C2)やデータ窃取のためのトンネリング手段として悪用される

検出の回避

約80%のマルウェアはC2サーバの識別にDNSを利用

ドメイン量には制限がない

マルウェアがDGAを利用する事で、従来に比べ対策が圧倒的に困難に

DGA・・・ドメイン生成アルゴリズム

DNS セキュリティ: 機械学習を活用した攻撃の阻止

あらたな悪性
ドメインの識別

DNSベースの
C2検出とDNS
トンネリングの
無力化

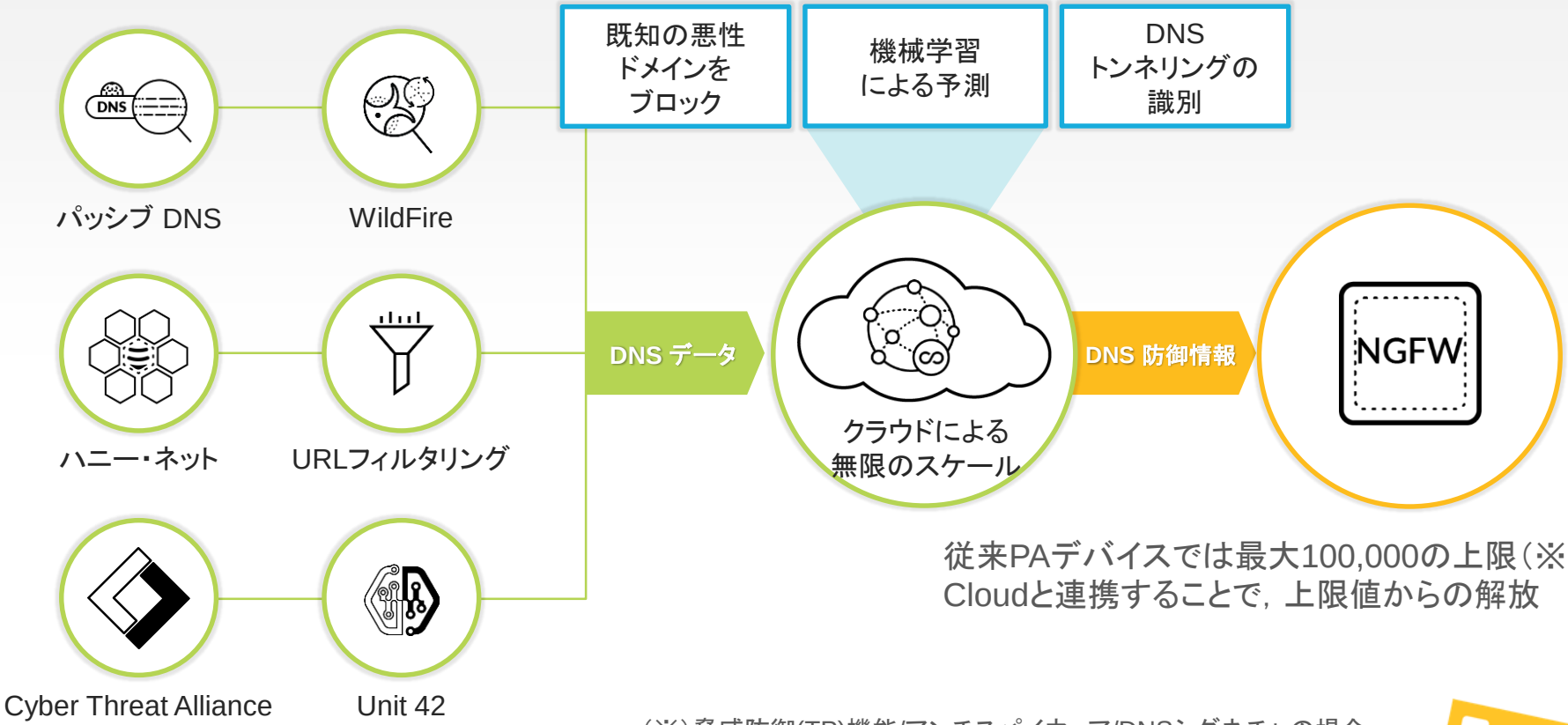
機械学習による予測

”悪い”ドメインと
C2の防止

感染ホストを
特定し封じ込める

オートメーションによる攻撃の防止

膨大なDNSデータを活用した機械学習によりDNS脅威からの保護を強化

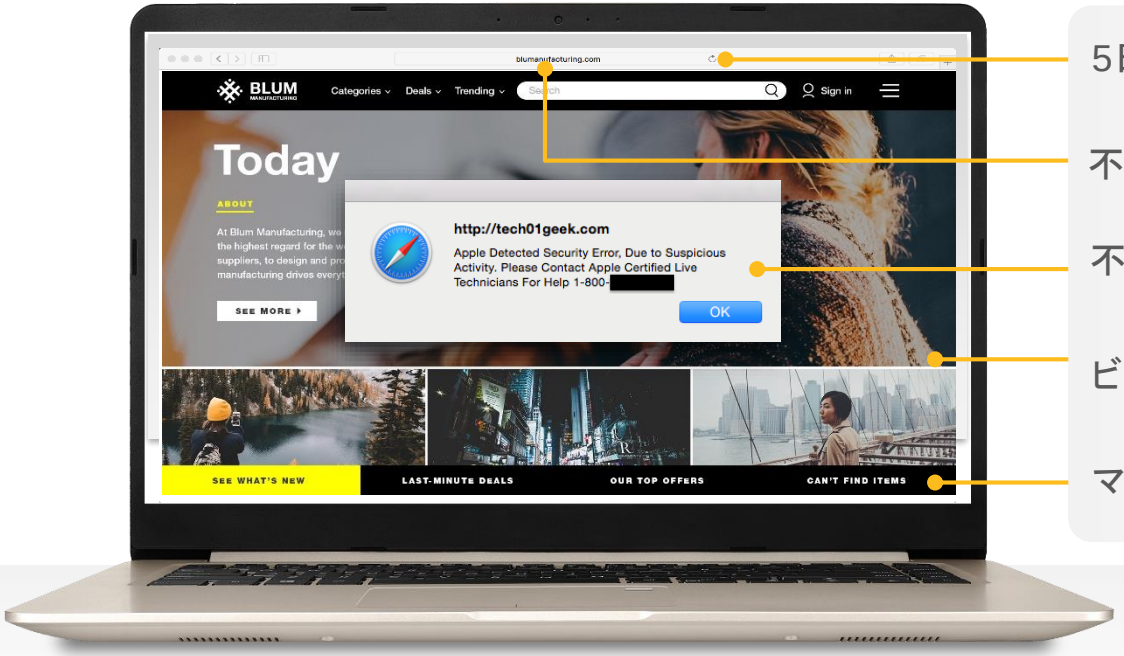


従来PAデバイスでは最大100,000の上限（※）
Cloudと連携することで，上限値からの解放

（※）脅威防御(TP)機能/アンチスパイウェア/DNSシグネチャの場合

URLフィルタリング機能の進化

URL フィルタリング: あたらしいカテゴリ分析



5日前に登録されたドメイン

不審な URL

不審なコンテンツ

ビジネス & 経済

マーケティングコンテンツ

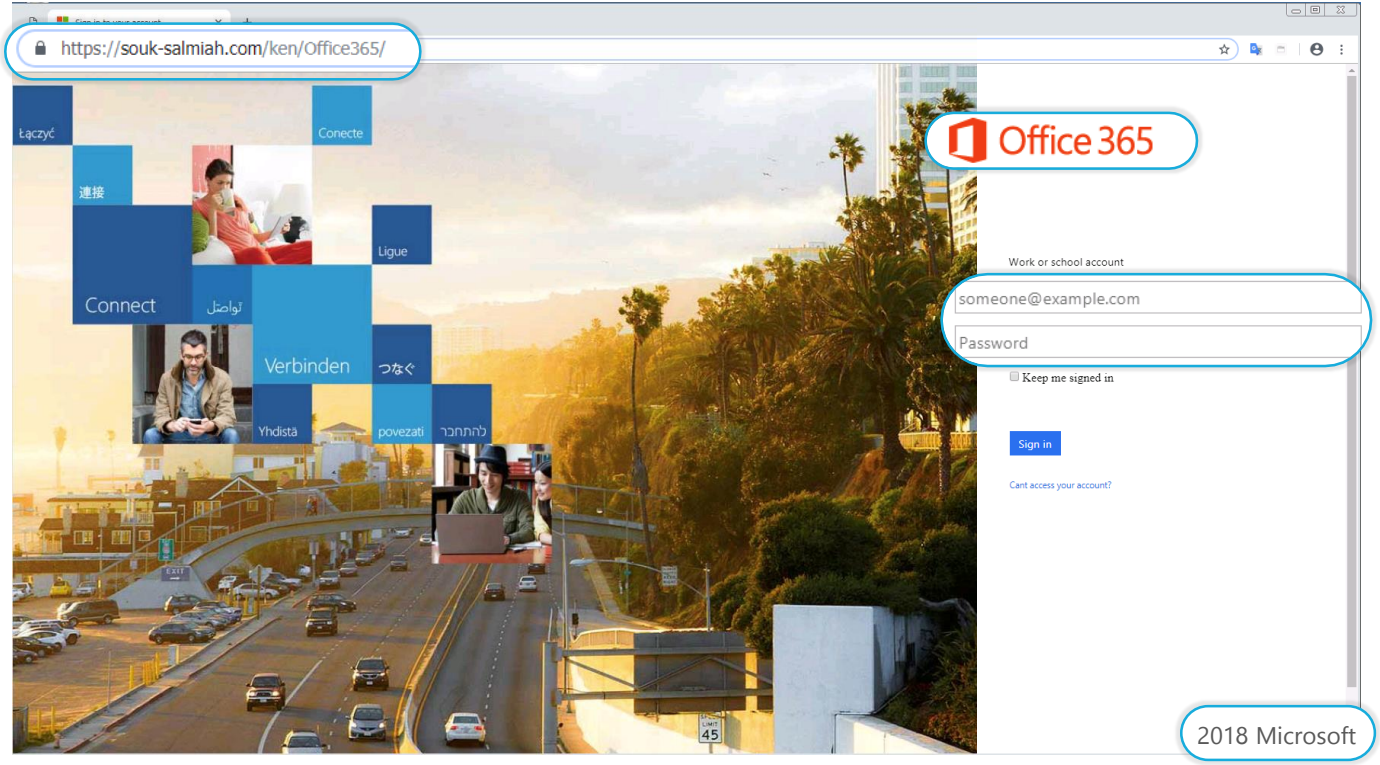
リスクベースによるカテゴリー

リスクレベル | 最近登録されたドメインかどうか？ | ダイナミックDNS

リスクベースカテゴリ

カテゴリ	判別方法
High-Risk	以前マルウェア，フィッシングサイトとして立証されたサイト．または，30日以内でC2サイトとして活動をしていたことのあるサイト
	PAN-DBがCategorize完了するまでの未知のドメイン
	Maliciousサイト．例) 特定のサイト自身がmaliciousでなくても，そのページないしは同じドメインにmaliciousホストが存在する場合　等
	ダークウェブ，違法サイト等にサービスを提供しているISP
	IPだけのサイト
Medium-Risk	すべてのCloudストレージのサイト
	以前マルウェア，フィッシングサイトとして立証されたサイト．または，過去60日でC2サイトとして活動をしていたことのあるサイト
	PAN-DBがCategorize完了するまでの未知のIPアドレス
Low-Risk	上記Riskカテゴリに分類されなかったコンテンツ
Newly-Registered Domains	直近32日以内で新たに登録されたサイト

URL フィルタリング: 継続的で高度なフィッシングサイト検知技術



あたらしいイメージ認識

機械学習ベースのディープラーニングにより、検知を回避するフィッシングを阻止

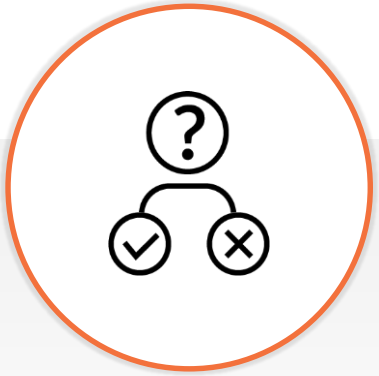
協調分析

より正確にあたらしいタイプのフィッシングページを特定

ポリシー最適化機能

従来型ポートベースのルールに関する問題

不必要なポート開放による
セキュリティリスクの増大



誤った設定による
危険性の増大

管理とトラブルシューティングのための時間の浪費

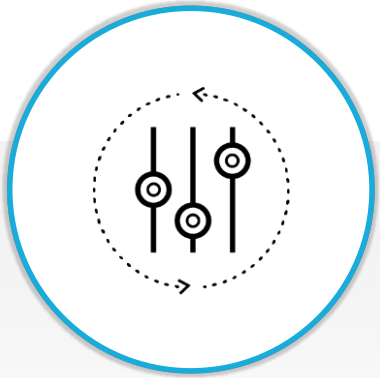
ポリシー最適化機能を使用した App-ID ベースのポリシーへの移行

セキュリティリスクの増大
不必要なオープンポートによる

より強力なセキュリティ:
App-ID利用によるギャップの解消

設定ミスの発生
頻繁な手動設定変更に伴う

エラー発生の最小化:
代表的な情報漏洩の原因



多くの時間の浪費
管理やトラブルシューティングに伴う

時間の節約
直感的なルールによる

ポリシーオプティマイザー画面での従来のルール

Policies

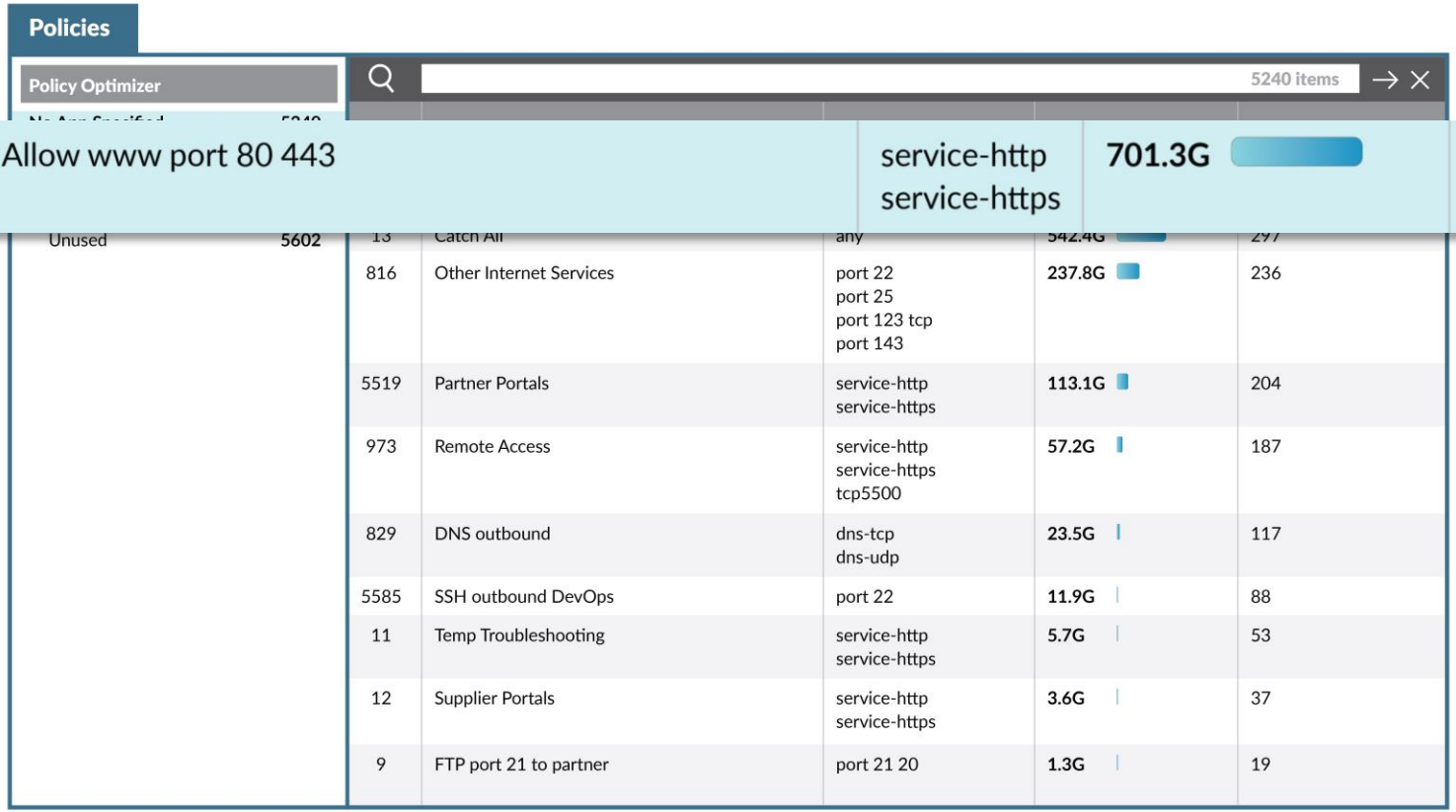
Policy Optimizer

No App Specified	**5240**
Unused Apps	**0**
Rule Usage	
Unused in 30 Days	**5604**
Unused in 90 Days	**5602**
Unused	**5602**

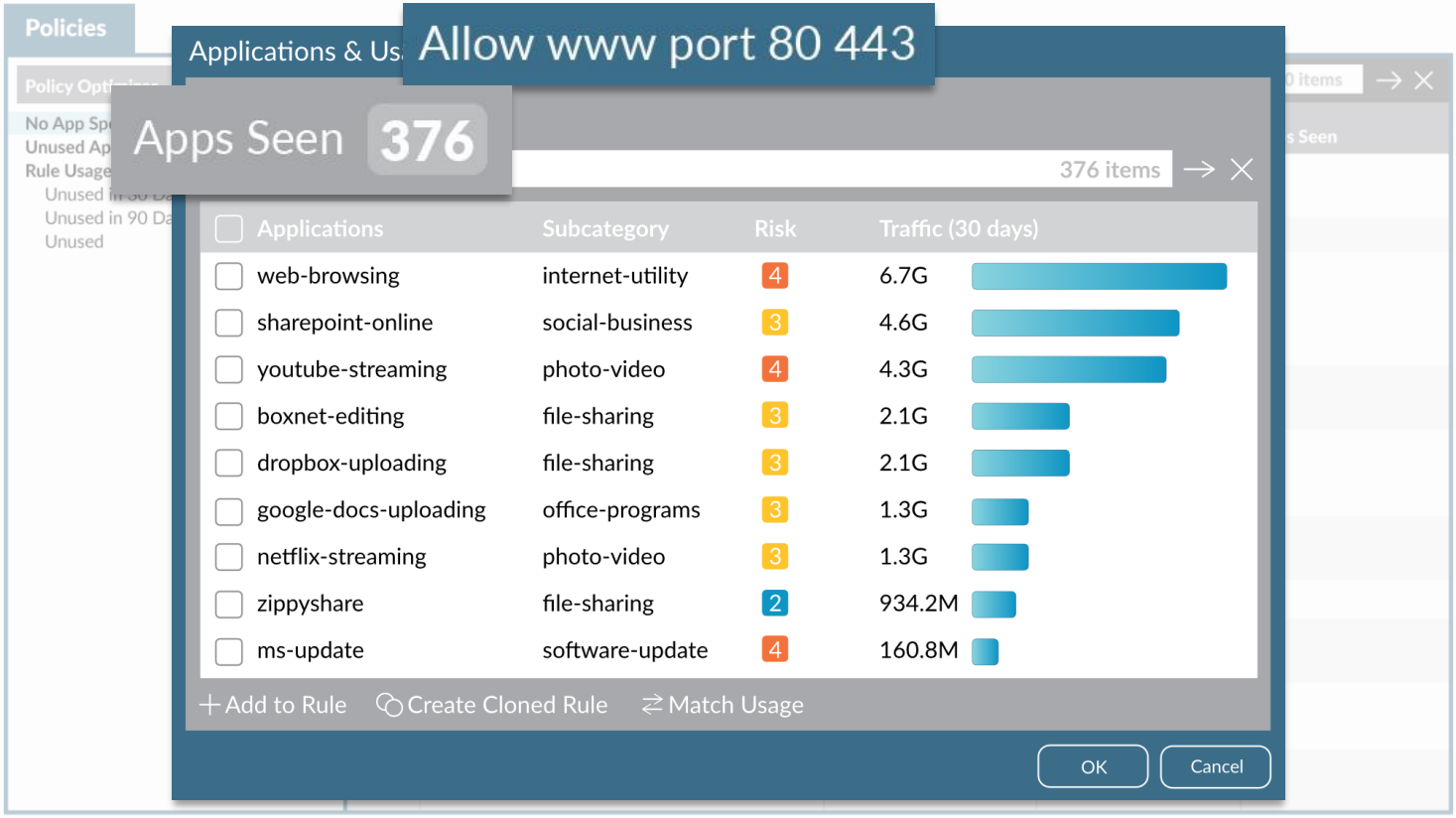
5240 items

	Name	Service	Traffic (Bytes, 30 days)	Apps Seen
4	Allow www port 80 443	service-http service-https	**701.3G**	376
13	Catch All	any	**542.4G**	297
816	Other Internet Services	port 22 port 25 port 123 tcp port 143	**237.8G**	236
5519	Partner Portals	service-http service-https	**113.1G**	204
973	Remote Access	service-http service-https tcp5500	**57.2G**	187
829	DNS outbound	dns-tcp dns-udp	**23.5G**	117
5585	SSH outbound DevOps	port 22	**11.9G**	88
11	Temp Troubleshooting	service-http service-https	**5.7G**	53
12	Supplier Portals	service-http service-https	**3.6G**	37
9	FTP port 21 to partner	port 21 20	**1.3G**	19

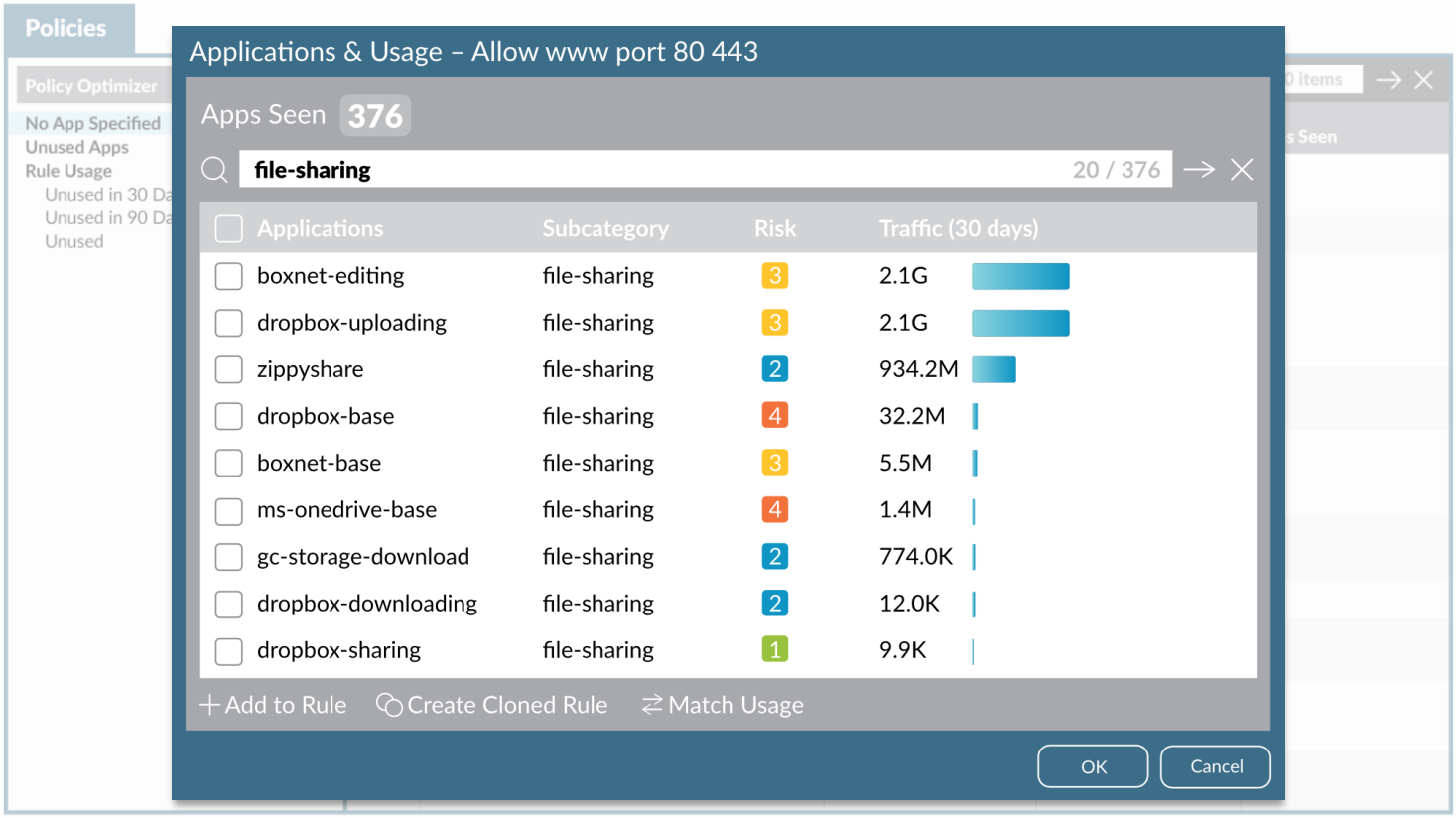
STEP 1: 最適化する既存ルールを選択



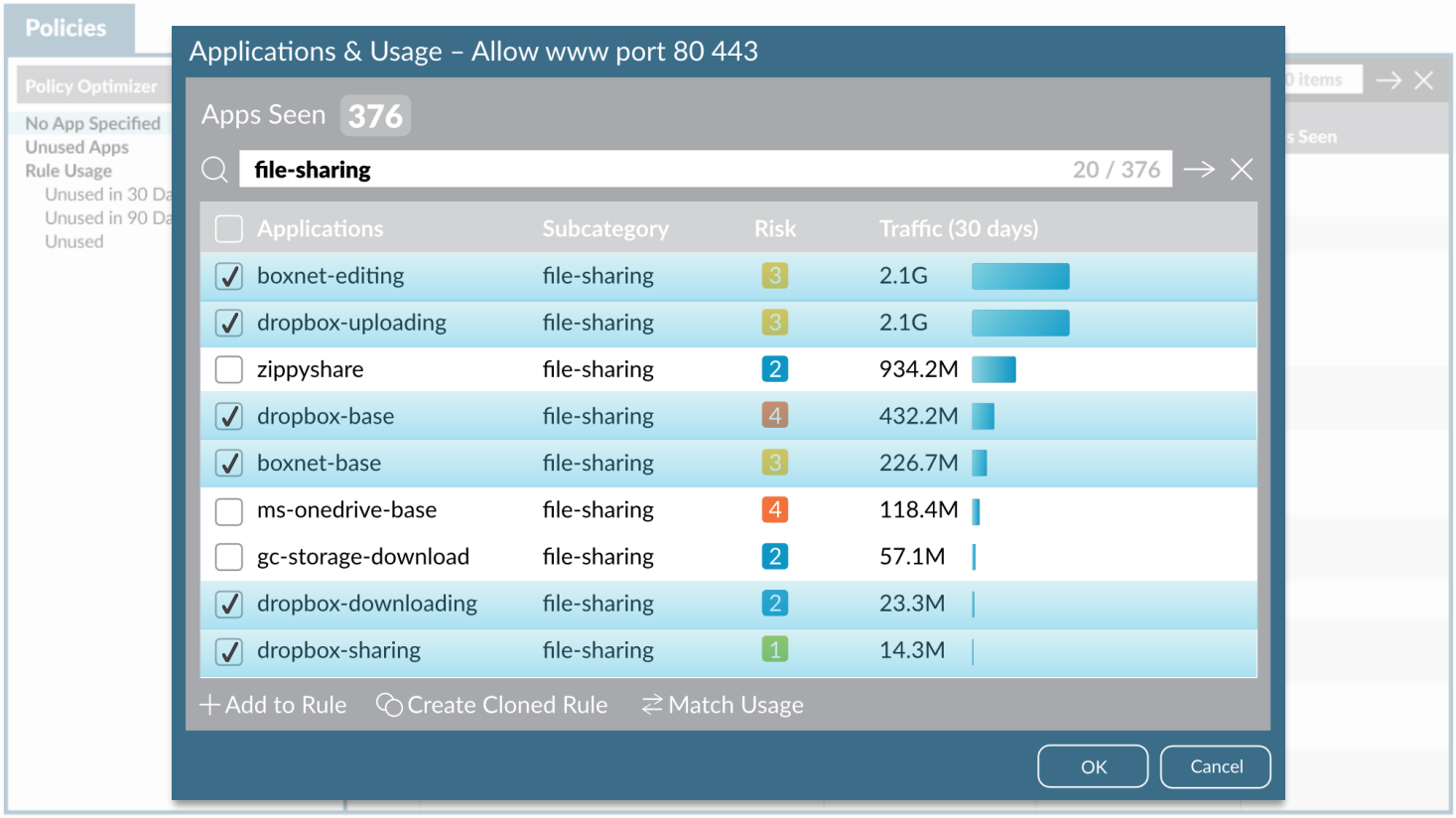
STEP 2: そのルールにマッチしているアプリケーションを表示



STEP 3: ファイル共有アプリケーションのフィルタリング例



STEP 4: 利用を許諾するアプリケーションを選択



アプリケーションベースのルール生成

	Name	Source User	[illegible]	Service	[illegible]	[illegible]
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow

Policies

Policy Optimizer	
No App Specified	5240
Unused Apps	0
Rule Usage	
Unused in 30 Days	5604
Unused in 90 Days	5602
Unused	5602

	Name	Service	Traffic (Bytes, 30 days)	Hit Count
4	Allow www port 80 443	service-http service-https	0	0

最終形：App-IDベースで最適化されたポリシー

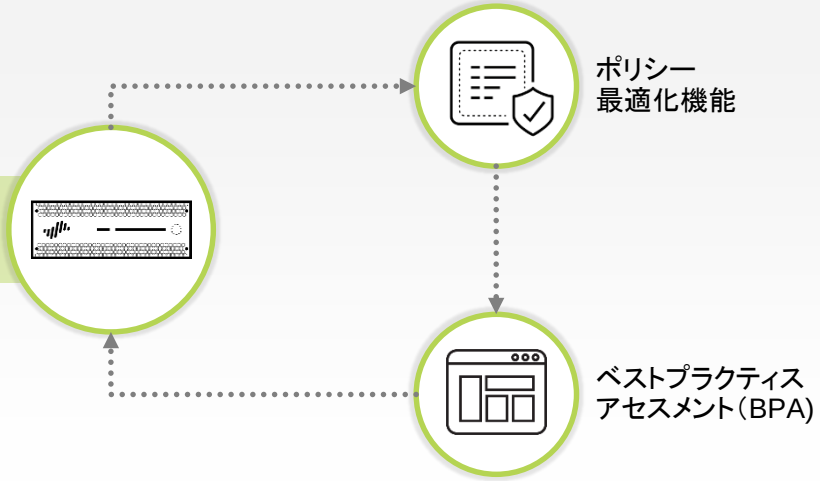
70 items

	Name	Source User	[illegible]	Service	[illegible]	[illegible]
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow
2	Tolerated SaaS Apps	corp-users contractors	docusign evernote google-base google-cloud-storage google-docs	application-default		Allow
3	Approved Social Media	marketing	facebook glassdoor linkedin twitter	application-default		Allow
4	Approved Web Email	corp-users	gmail icloud yahoo-mail	application-default		Allow
5	Software Updates	corp-users marketing contractors	apple-update google-update java-update ms-update paloalto-updates	application-default		Allow
6	Other Web Traffic URL Filtering	corp-users contractors	ssl web-browsing	application-default		Allow

従来型ポリシーからApp-IDベースへのポリシー移行による保護の強化

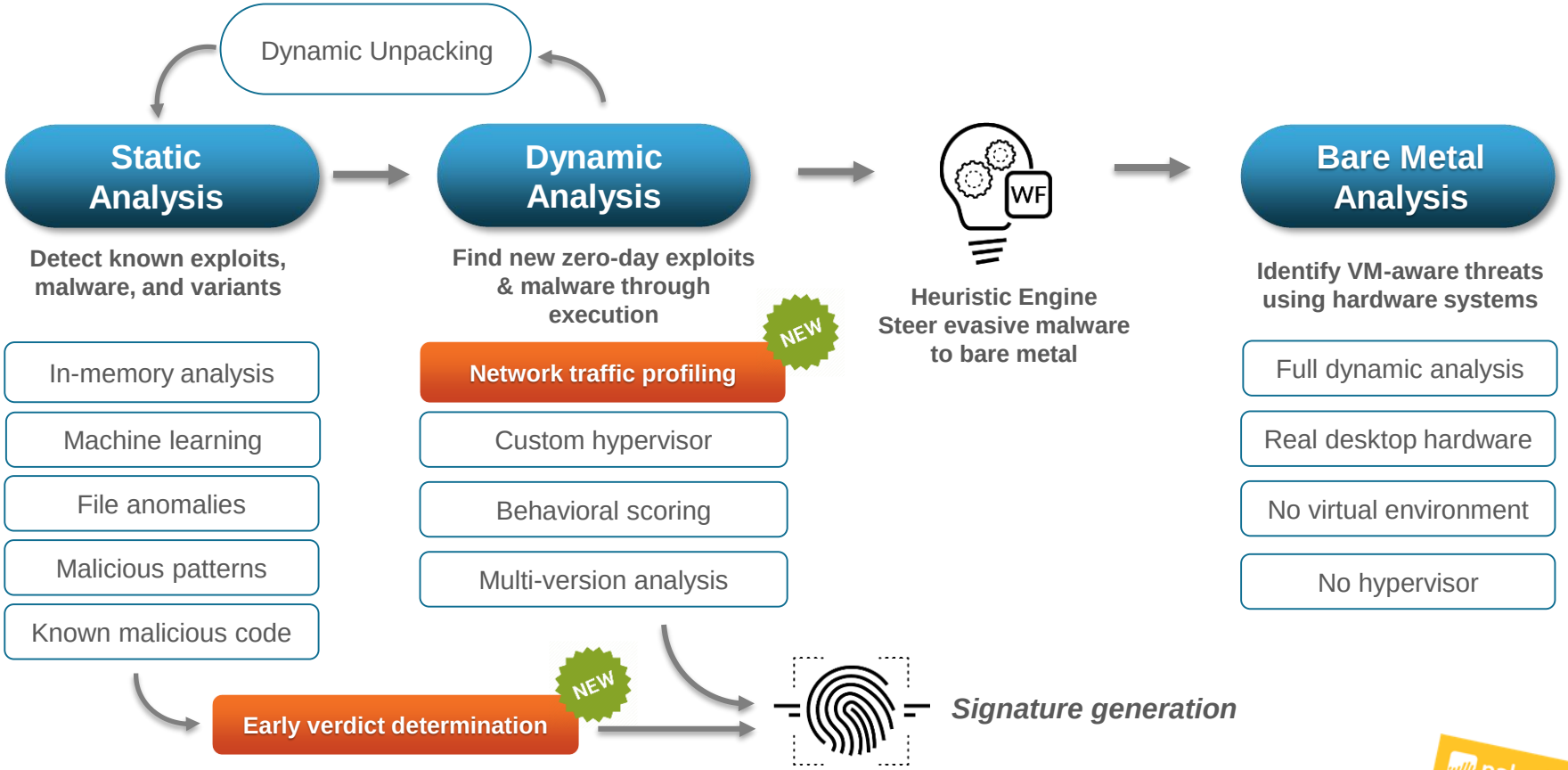
1. マイグレーションツールを使用し、従来型FWから次世代ファイアウォールへルールを移行

2. ベストプラクティスアセスメント(BPA)とポリシー最適化機能を使用した継続的な保護プロセス



WildFireの進化

WildFire クラウド分析エンジンの進化



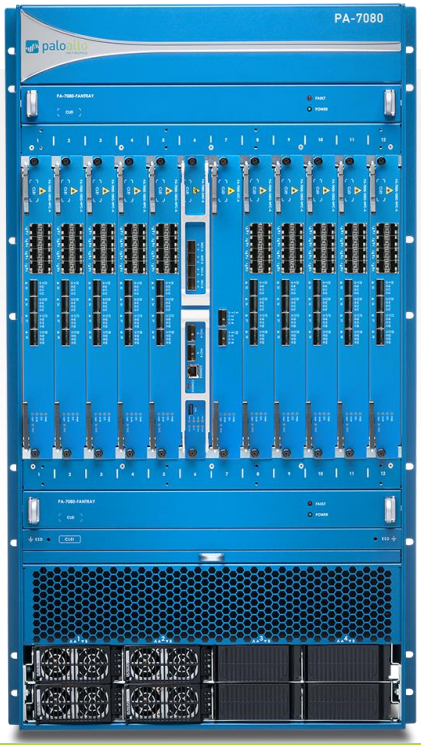
WildFireへのファイルアップロード制限の拡張

ファイルタイプ	OS9.0以前	OS9.0以降
pe	16MB	1 - 50MB
apk	10MB	1 - 50MB
pdf	3,072KB	100 - 51,200KB
Ms-office	16,384KB	200 - 51,200KB
jar	5MB	1 - 20MB
flash	5MB	1 - 10MB
MacOSX	10MB	1 - 50MB
archive	50MB	1 - 50MB
linux	50MB	1 - 50MB

新ハードウェア

業界史上最速の性能を誇る次世代ファイアウォール

- **350 Gbps 脅威防御スループット:**
  競合他社を上回る約2倍の性能
- 復号化パフォーマンスが3倍、
  復号化セッション容量が25倍*
- **100Gと40Gの接続オプション**
- **既存設備の有効活用:**
  既存のシャーシであたらしいカードが使用可能



セキュリティを犠牲にすることなくパフォーマンスを拡張

**第一世代のNPCと比較*

新ハードウェア

- PA-7kシリーズに以下のモジュールを追加
  - New SMC
    - Mobile系プロトコル（GTP）サポート
  - LFC：Log Forwarding Card
    - 従来のLPC（Log Processor Card）から変更.
    - ログを外部へForwardingさせるモジュール
  - NPC
    - 8 x SFP/ SFP+ & 4 x QSFP/ QSFP28モジュール
      - ターゲットパフォーマンス
        - App-ID：100Gbps（100Gbps/ AppOverride）
        - Threat：30Gbps
- GTPプロトコルをサポートさせるためには，New SMC/ LFCへ変更する必要あり
  - アップグレード用SKUを準備予定

その他アップデート

PAN-OS 9.0: 60を超える新機能

App-ID
- Policy Optimizer
- HTTP/2 inspection
- SIP enhancements
- App-default with decryption

User-ID
- Increased terminal services capacity
- Improved scalability with virtual systems

脅威防御
- New DNS Security Service
- Multi-dimensional URL filtering
- Realtime URL category updates
- EDL capacity and performance improvements
- GTP security for IoT
- More flexible data filtering

新ハードウェア
- PA-7000 Series: New cards

Panorama
- Manage up to 5,000 NGFWs with single Panorama instance; up to 30,000 NGFWs with Panorama Interconnect
- Device group/template config management
- Optimized bulk onboarding of NGFWs

マネージメント
- Dynamic Address Groups: increased capacity, performance, and visibility
- API security
- API simplification
- Wildcard Address Support for policy match
- Rule audit comments
- Tag-based rule management
- Policy/infrastructure testing in UI
- Policy UUID

GlobalProtect
- Managed/unmanaged device identification
- HIP redistribution

ネットワーク
- DHCP/FQDN support for dest NAT
- FQDN refresh responsiveness improvement
- VxLAN inspection
- GRE tunneling
- TrustSec SGT Tag support

WildFire
- Larger file size support
- Rapid analysis and signature generation
- Network traffic profiling and analysis
- FedRAMP-ready designation
- New file types (scripts, tar, cab, dex)

VM シリーズ
- Oracle Cloud, Alibaba Cloud, Nutanix, Cisco ENCS support
- Up to 2.5x performance increase on AWS and Azure
- Plugin architecture on VM-Series

AutoTagによる自動制御

AutoTagによる自動制御とは？

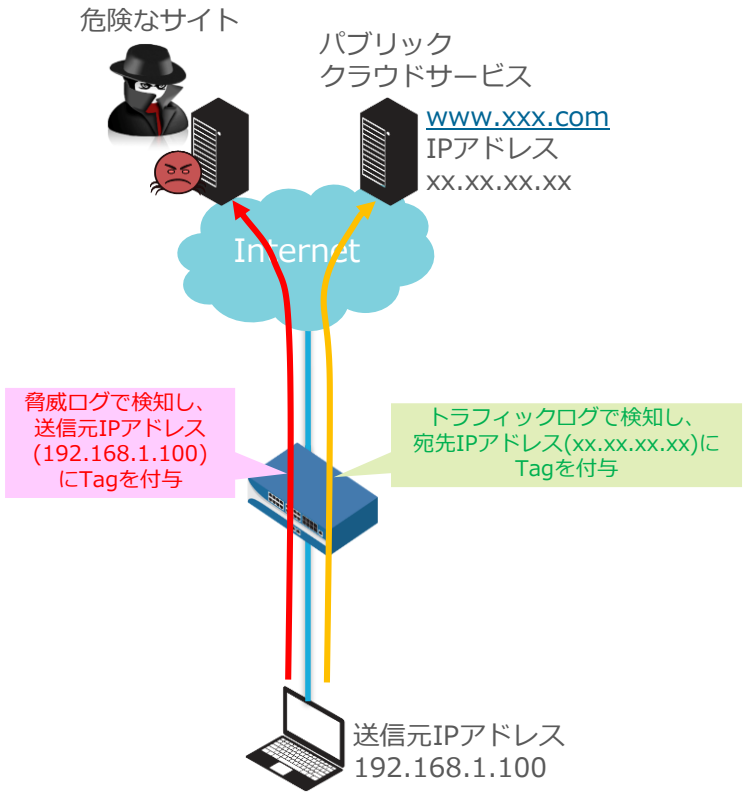
PAN-OS 8.0で追加された機能

- トラフィックログや脅威ログ、URLフィルタリングログなどを**ログをトリガー**に、検知した通信の送信元IPアドレスもしくは宛先IPアドレスに**タグを自動的に付与**、もしくは削除する機能
- Tagと連携するダイナミックアドレスグループを利用し、動的にポリシー適応が可能

PAN-OS 9.0にてタイマー機能が追加

- AutoTagで付与されたタグにタイマー機能が付き、設定した時間が経過すると自動的にタグが削除

（※）PAN-OS 8.1までは自動的にタグは削除されず、管理者がGUI/CLIで手動で削除、もしくはログ転送プロファイルで特定のログをトリガーにタグを削除。



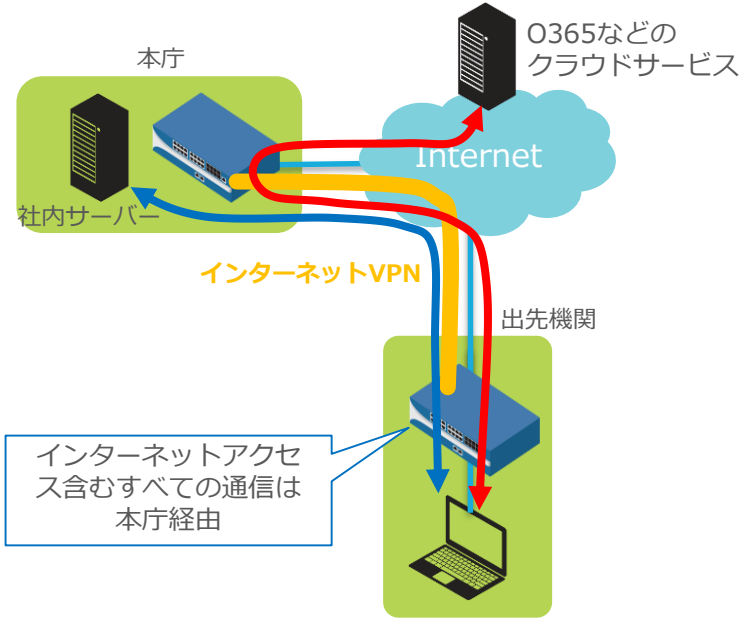
AutoTagによる自動制御の利用例

1. マルウェアファイルのダウンロード、アンチスパイウェアでC2通信検知など、いずれかの条件に該当する端末を**自動的にインターネットの全遮断**。
   - 脅威ログで検知された場合、送信元IPアドレス(=クライアントのIPアドレス)にタグをつける
2. Windowsアップデート通信をポリシーベースフォワーディング(PBF)で**自動的に回線制御**(※インターネット回線が複数回線ある場合)
   - App-IDのトラフィックログでms-updateを検知した場合、その送信先IPアドレス(=Windowsアップデートで利用されているサーバーのIPアドレス)にタグをつける
3. 端末のOS種別により**適応するポリシーを自動で適応**
   - URLフィルタリングログのUser-Agent情報より、送信元IPアドレス(=クライアントIPアドレス)に端末のOSに該当するにタグをつける

AutoTagを利用したアプリケーション単位でのインターネットブレイクアウト

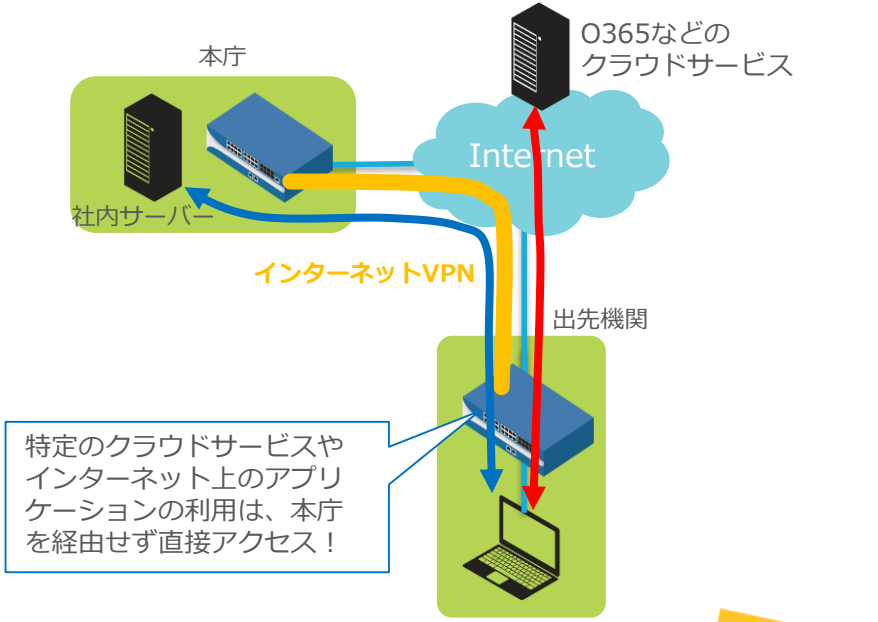
■インターネットVPNの課題

支店からクラウドサービス利用時に、本庁を経由するため本庁のインターネット回線を圧迫し、レスポンス低下を招く。
解消するには本庁の回線増強やインターネットVPN装置のアップグレードが必要

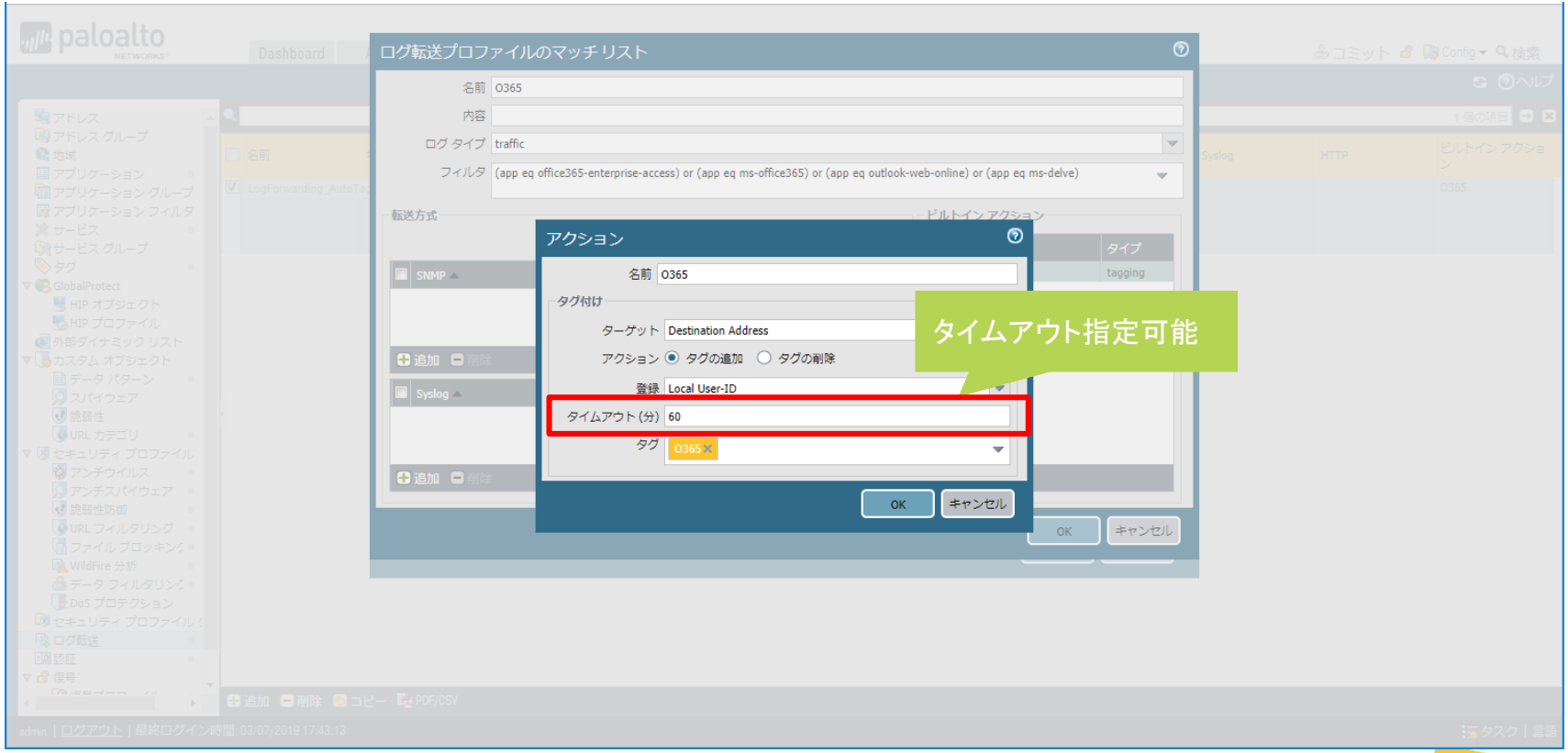


■インターネットブレイクアウトによる解決

特定のクラウドサービスやインターネット上のアプリケーションの利用に関しては、本庁を経由せず直接インターネットをアクセス。
（タグが付くまでは本庁経由。タグが付いた時点からブレイクアウトし、支店から直接アクセス）



【PAN-OS 9.0新機能ご紹介】　AutoTagにタイムアウト機能追加



【PAN-OS 9.0新機能ご紹介】　IP-Tagのログ機能


paloalto
NETWORKS®