

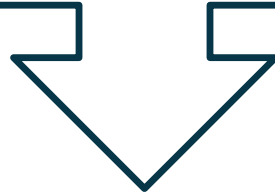
Security Policy最適化のススメ

パロアルトネットワークス(株)



セキュリティ機器の不安？

- ハードウェアサポート切れに伴う懸念事項
 - 従来から使用しているファイアウォールに設定されているPolicyをどうする？
- 日々の運用
 - 日々進化する攻撃に対してどう守っていくか？



- セキュリティ機器のリプレイス(交換)時には従来使用しているPolicyを移植
- 日々の攻撃防御の際のPolicy変更/ 追加/ 削除

これらをまとめると...

- コスト面の懸念
 - Policy移植による設定変更費
 - 移植を繰り返すと、機器のPolicy設定数上限値に到達し、上位機種を選択する状況へ？
 - Policy 変更/ 追加/ 削除等をおこなうためのオペレータ教育費
- 人的リソースの懸念
 - Security専任のオペレータ不足
 - 定期Policyのメンテナンス
 - 何が不要で何が必要なPolicyなのか？
 - 適切なトラフィック制御が行われているか？

欧米と日本の文化の違い

欧米

1. ログ統合管理装置による監視
2. 予兆の検知と対策の検討
3. 検討シナリオに基づくセキュリティデバイスへの適用/チューニング

セキュリティスペシャリストによる警備体制の確立

日本

1. ログ統合管理装置による監視
 - ・ 実際には蓄積のみ？
2. 予兆の検知と対策の検討
 - ・ 実は周りの情報に依存？
3. 検討シナリオに基づくセキュリティデバイスへの適用/チューニング
 - ・ 実はIntegratorにお任せ？

IT担当者がセキュリティも兼務

正しいセキュリティPDCAサイクルを作るために...

- ・ 国のガイドライン・政策と併せた全国的な意識改革
- ・ 必要などころに必要な予算を！
- ・ CISO、IT・セキュリティ、ネットワーク担当の配備と連携
- ・ 自動化ツールの導入

これらを踏まえて...

- 最初の一步:リプレース時のPolicy移植の自動化
 - Policy移植ツール: Expedition
 - 以下メーカーからPAシリーズへの設定にマイグレーションするツール
 - Checkpoint、Juniper、Cisco、IBM、Forcepoint、Fortinetからのマイグレーションをサポート
 - 移植後のトラフィックログを使ってPolicyの最適化
 - マシンラーニング機能による精度の向上

The screenshot displays the Expedition web interface. At the top, there is a navigation menu with tabs for DASHBOARD, IMPORT, PLUGINS, BEST PRACTICES, M.LEARNING, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, TOOLS, and EXPORT. The 'IMPORT' tab is active. Below the navigation, there are tabs for different vendors: PALO ALTO, CSV, CHECKPOINT, CISCO, FORTINET, IBM XGS, JUNIPER, and FORCEPOINT. The 'PALO ALTO' tab is selected. The main content area is divided into two sections: 'Single File' and 'Multiple Files (in ZIP)'. The 'Single File' section has a description: 'Upload a Panos or Panorama configuration XML file. Export it from your device.' and a text input field for 'XML File' with a 'Browse' button. The 'Multiple Files (in ZIP)' section has a description: 'Upload a ZIP file with all the configurations to import' and a text input field for 'ZIP File' with a 'Browse' button. Below this, there are tabs for 'DEVICES' and 'SNIPPETS'. The 'DEVICES' tab is active, showing a table with the following data:

Image	Name	Hostname	Serial #	Port	Type	Panos	Description
	VMSeriesFW	10.30.11.1	007051000019156	443	vm-series	8.1.1	

移植後、次の二歩

- 移植しただけでは、最適化がなされていない。不要/ 必要なPolicyの精査が必要
- Rule Hit Counter(PANOS8.1より)によるPolicyの使用/ 不使用の確認

- 使用されているPolicyは、カウントアップ
- 最初/ 最後にヒットした日時が記録
例; 下記Policyでは...
 - #4、7、8のPolicyは一度もヒットしないため、不要と判断できる?
 - Disable/ 削除をしてみよう!











名前	タグ	Type	送信元					宛先		ルールの使用状況			アプリケーション	サービス
			Zone	アドレス	User	HIP プロファイル	Zone	アドレス	ヒット数	最後のヒット	最初のヒット			
1	clear	none	universal	vwire	any	any	any	vwire	any	16184	2018-04-17 15:32:39	2018-02-01 14:52:49	any	applic
2	fb0	none	intrazone	vwire	any	any	any	(intrazone)	any	55	2018-02-01 14:51:36	2018-02-01 14:48:54	web-browsing	applic
3	fb1	FB_test	intrazone	vwire	any	any	any	(intrazone)	any	1282	2018-02-01 14:52:01	2018-02-01 14:49:33	facebook-base	applic
4	fb1.5	FB_test	intrazone	vwire	any	any	any	(intrazone)	any	0	-	-	facebook-chat	applic
5	fb2	FB_test	intrazone	vwire	any	any	any	(intrazone)	any	2888	2018-02-01 14:57:10	2018-02-01 14:46:14	any	any
6	rule1	none	universal	trust	any	any	any	untrust	any	467	2018-01-25 12:18:24	2017-12-22 13:31:27	any	any
7	test1	none	universal	vrf1	any	any	any	vrf2	any	0	-	-	any	any
8	test2	none	universal	vrf2	any	any	any	vrf1	any	0	-	-	any	any
9	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	13	2018-04-15 15:13:41	2018-02-22 11:23:55	any	any
10	interzone-default	none	interzone	any	any	any	any	any	any	0	-	-	any	any

その次の日々の運用

- PANOS9.0からPolicy Optimizer機能がサポート
 - Policy Optimizerでできること
 - 実際に流れているトラフィックを基にアプリケーションレベルでPolicyの最適化が可能

Policies		Policy Optimizer			
Policy Optimizer		5240 items			
No App Specified	Unused Apps	Rule Usage			
5240	0	Unused in 30 Days	5604		
		Unused in 90 Days	5602		
		Unused	5602		
Name	Service	Traffic (Bytes, 30 days)	Apps Seen		
4	Allow www port 80 443	701.3G	376		
13	Catch All	542.4G	297		
816	Other Internet Services	237.8G	236		
5519	Partner Portals	113.1G	204		
973	Remote Access	57.2G	187		
829	DNS outbound	23.5G	117		
5585	SSH outbound DevOps	11.9G	88		
11	Temp Troubleshooting	5.7G	53		
12	Supplier Portals	3.6G	37		
9	FTP port 21 to partner	1.3G	19		

Policy Optimizer (Step1)

Policies		Policy Optimizer					
Policy Optimizer		Q		5240 items	→ X		
No App Specified	5240		Name	Service	Traffic (Bytes, 30 days)	Apps Seen	
Unused Apps	0		4	Allow www port 80 443	service-http service-https	701.3G 	376
Rule Usage			13	Catch All	any	542.4G 	297
Unused in 30 Days	5604		816	Other Internet Services	port 22 port 25 port 123 tcp port 143	237.8G 	236
Unused in 90 Days	5602		5519	Partner Portals	service-http service-https	113.1G 	204
Unused	5602		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

Policy Optimizer (Step2)

Policies

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

5240 Items → ×

	Name	Service	Traffic (Bytes, 30 days)	Apps Seen
4	Allow www port 80 443	service-http service-https	701.3G <div style="width: 100%; height: 10px; background-color: #0070c0; border-radius: 5px;"></div>	376
5519	Partner Portals	port 143 service-http service-https	113.1G <div style="width: 100%; height: 10px; background-color: #0070c0; border-radius: 5px;"></div>	204
5585	SSH outbound DevOps	port 22	11.9G <div style="width: 100%; height: 10px; background-color: #0070c0; border-radius: 5px;"></div>	88
11	Temp Troubleshooting	service-http service-https	5.7G <div style="width: 100%; height: 10px; background-color: #0070c0; border-radius: 5px;"></div>	53
12	Supplier Portals	service-http service-https	3.6G <div style="width: 100%; height: 10px; background-color: #0070c0; border-radius: 5px;"></div>	37
9	FTP port 21 to partner	port 21 20	1.3G <div style="width: 100%; height: 10px; background-color: #0070c0; border-radius: 5px;"></div>	19

4

Allow www port 80 443

service-http
service-https

701.3G

376

現在ポート番号80、443をAllowとしているPolicyを最適化する

Policy Optimizer (Step3)

Applications & Usage – Allow www port 80 443

Apps Seen **376**

Q 376 items → X

<input type="checkbox"/> Applications	Subcategory	Risk	Traffic (30 days)
<input type="checkbox"/> web-browsing	internet-utility	4	6.7G
<input type="checkbox"/> sharepoint-online	social-business	3	4.6G
<input type="checkbox"/> youtube-streaming	photo-video	4	4.3G
<input type="checkbox"/> boxnet-editing	file-sharing	3	2.1G
<input type="checkbox"/> dropbox-uploading	file-sharing	3	2.1G
<input type="checkbox"/> google-docs-uploading	office-programs	3	1.3G
<input type="checkbox"/> netflix-streaming	photo-video	3	1.3G
<input type="checkbox"/> zippyshare	file-sharing	2	934.2M
<input type="checkbox"/> ms-update	software-update	4	160.8M

+ Add to Rule Create Cloned Rule Match Usage

実際に流れているトラフィックの状況を表示

Policy Optimizer (Step4)

The screenshot displays the 'Applications & Usage' section of the Palo Alto Networks Policy Optimizer. The title is 'Applications & Usage - Allow www port 80 443'. It shows a search filter for 'file-sharing' with 20 items out of 376 total apps seen. A table lists various applications with their subcategories, risk levels, and traffic volumes over 30 days. Checkmarks in the left column indicate which applications are selected for the policy.

<input type="checkbox"/>	Applications	Subcategory	Risk	Traffic (30 days)
<input checked="" type="checkbox"/>	boxnet-editing	file-sharing	3	2.1G
<input checked="" type="checkbox"/>	dropbox-uploading	file-sharing	3	2.1G
<input type="checkbox"/>	zippyshare	file-sharing	2	934.2M
<input checked="" type="checkbox"/>	dropbox-base	file-sharing	4	432.2M
<input checked="" type="checkbox"/>	boxnet-base	file-sharing	3	226.7M
<input type="checkbox"/>	ms-onedrive-base	file-sharing	4	118.4M
<input type="checkbox"/>	gc-storage-download	file-sharing	2	57.1M
<input checked="" type="checkbox"/>	dropbox-downloading	file-sharing	2	23.3M
<input checked="" type="checkbox"/>	dropbox-sharing	file-sharing	1	14.3M

At the bottom of the table, there are three action buttons: '+ Add to Rule', 'Create Cloned Rule', and 'Match Usage'.

“file-sharing”トラフィックのみでフィルタし、更に特定アプリケーションのみをAllowとする

Policy Optimizer (Step5)

70 items						
	Name	Source User	Application	Service	Security Profile	Action
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365	application-default		Allow

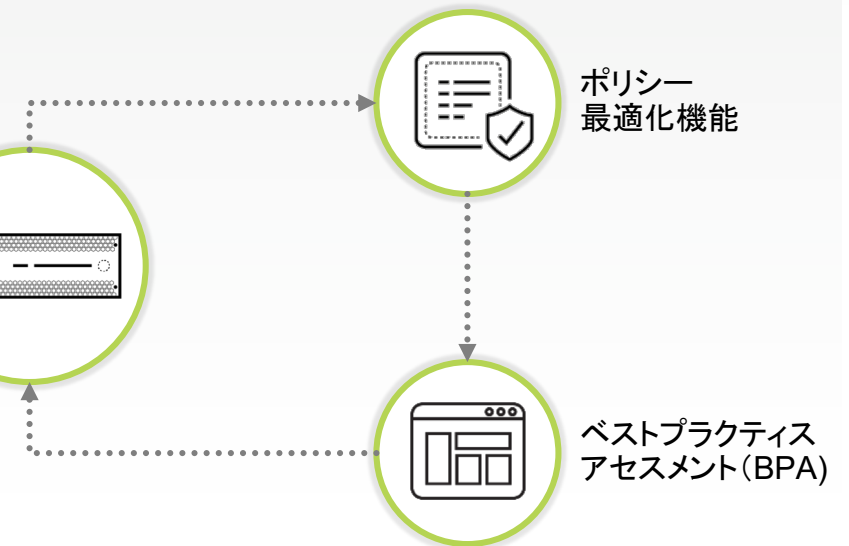
	Name	Source User	Application	Service	Security Profile	Action
1	Sanctioned SaaS Apps	corp-users	boxnet concur confluence dropbox jira ms-office365 slack	application-default		Allow
4	Approved Web Email	corp-users	gmail icloud yahoo-mail	application-default		Allow
5	Software Updates	corp-users marketing 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



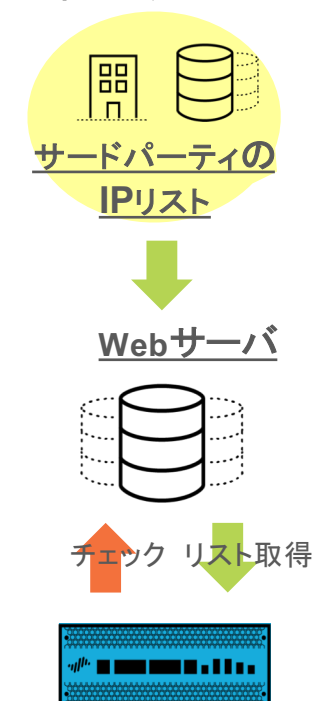
2. ベストプラクティスアセスメント(BPA)とポリシー最適化機能を使用した継続的な保護プロセス



おまけ
日々の運用で有効な様々な機能

External Dynamic List

- External Dynamic List(以降EDL)とは、以下の情報を指定したURLから動的に取得し、ブラック/ ホワイトリストとして動的にPolicyへ適用する機能
 - Dynamic IP List
 - Dynamic Domain List
 - 後述DNSシンクホール機能で利用
 - Dynamic URL List
 - カスタムURLカテゴリで使用
- デバイス毎に最大30まで設定可能
- 取得した情報を反映させるためのCommit処理は不要
- デバイスで保持可能なリスト数



	PA 7K	PA 7K (XM)	PA 5200 series	PA 3200 series	PA 800 series	VM-500/700	VM-300	Others
Domains	500K	4M	4M	1M	1M	2M	500K	50K
URLs	100K	250K	250K	100K	100K	100K	100K	50K

Malicious IP Address Feeds (PANOS8.0より)

- EDLにて、以下の2つのPre-definedのIP feedリストを提供
 - つまり、IP ブラックリストのフィード
 - Known malicious IP addresses
 - PaloAlto Networksの脅威分析チームが確認済みのmalicious IPアドレスリスト
 - High Risk IP addresses
 - Maliciousな活動に関連したIPアドレスのリスト
 - 信頼出来る3rd パーティ/ 公的機関等から提供されたIPアドレスリスト
 - IP feedリストは毎日更新
 - 提供されるIP feedリストは随時追加予定
 - **Threat Preventionサブスクリプションが必要**



DNSシンクホール

- 内部DNSが存在する環境においても、内部の感染端末を特定する(感染端末のアドレス情報を把握する)
 - 内部にDNSが存在しない環境の場合は、DNS signatureにて感染端末の特定は可能

