

PA Series Firewall 設定ガイド(PAN-OS 8.1) V1.0

Palo Alto Networks K.K. 2018/4

1.	はじ	こめに	4
2.	ネッ	トワーク構成	5
3.	初其	朋設定	6
3	.1.	マネージメント IP の設定	
3	2	WFBUIへのアクセス	7
3	3	NSとNTPの設定	9
3	4	設定のコミット	
3	5	設たのコペクト	
3	6	シグネチャのダウンロードとインストール	14
3	.7.	OS アップグレード	
4.	ネッ		
1	1		21
4	ຳ. ວ	VIRTOAL WIRE 改足の別际	۰۰۰۰۰۲ ۲۵
4	۰.∠. م	ノーノの設定	22 22
4		インダーフェイへの設定	Zo
4	.4.		20
5.	NA.	Т	28
6.	全評	午可ポリシーの設定	30
6	.1.	「参考」「ルールの使用状況」カウンター	
6	.2.		
6	.3.		
7	661		24
1.	331	L/ILS 復考化の設定	
7	.1.	ルート証明書の生成	35
7	.2.	ルート証明書の用途設定	36
7	.3.	証明書のエクスポートとインボート	37
7	.4.	SSL/TLS 復号ポリシーの設定	41
7	.5.	通信確認	43
7	.6.	[参考] 「信頼されない証明書」の場合には必ずセキュリティ警告を出す設定	46
7	.7.	信頼されない証明書を持つサイトとの通信をブロック	54
7	.8.	[参考]そもそも「信頼された証明書」や「信頼されない証明書」とは?	56
7	.9.	一部の URL カテゴリを復号化から除外する	57
8.	コン	フフィグの操作	62
8	.1.	スナップショットの保存	62
8	.2.	スナップショットのエクスポートとインポート	63
8	.3.	スナップショットのロード	64
9.	ネッ	トワーク構成の変更	65
9	.1.	変更後のネットワーク構成	
9	.2.	マネージメントインターフェイスの設定変更	
9	.3.	アップデートサーバーへの接続エラーを回避する方法	67
10	+	ナービスを阻定するポリシーの設定	70
10.		リーニスを限定するホリノーの設定	
1	0.1.	HTTPとHTTPSのみ許可する設定	
1	0.2.	INTERZONE-DEFAULT の設定変更	
11.	Α	APP-ID	75
1	1.1.	DNS を許可する	75
1	1.2.	「参考」 APPLICATION-DEFAULT とは	79
1	1.3.	NTP を許可する	80
1	1.4.	YouTubeを拒否する	82
1	1.5.	YouTube のストリーミングのみ許可する	85

11.6.	[参考]アプリケーションの依存関係	
11.7.	リスク5の FILE SHARINGをまとめて拒否する	
11.8.	リスク5の FILE SHARING のうち、一つだけ許可する	96
12. CC	ONTENT-ID	
12.1.	アンチウイルス	
12.2.	脆弱性防御	
12.3.	WILDFIRE	
12.4.	ファイルブロッキング	111
12.5.	アンチスパイウェア	
12.6.	URL フィルタリング	
12.7.	データフィルタリング	130
13. US	SER-ID	134
13.1.	設定	
13.2.	動作確認	139
14. お	わりに	141
15. 「考	またしていた。 参考) URL カテゴリの一覧	
Lø	·····	

1. はじめに

本ガイドにて、PA シリーズファイアウォール (以下、PA Firewall) の設定方法をご紹介します。

初めて PA Firewall を起動してから、最初に必要となるライセンス投入やシグネチャのダウンロード、OS のアップグレード 方法、ネットワーク設定、SSL 復号化、そして様々な脅威防御が行えるまでの、一通りの設定方法をまとめました。

PA Firewall には以下3つの特徴があり、それぞれの設定と動作確認の方法も記載しています。

- ① App-ID アプリケーションを識別
- Content-ID コンテンツを識別
- ③ User-ID ユーザーを識別

弊社提供の正式ドキュメントと併用して頂き、新規設置作業や日々の運用時の設定変更作業時の参考ドキュメントとして ご活用ください。

※) 以降の設定画面は PAN-OS 8.x を基にしています。
 適用する PAN-OS が異なる場合は、該当する OS のドキュメントを参照してください。

2. ネットワーク構成

以下のネットワーク構成を前提として、以降、PA Firewall の設定を行います。



- PA Firewall のマネージメントインターフェイスは、最初はインターネットへの直接接続が可能な構成とします。
 (後で Trust ゾーンのネットワークに接続変更します。)
- PA Firewall に以下 2 つのゾーンを設定し、この 2 つゾーン間のポリシー設定を行います。
 - O Untrust ゾーン: インターネット側 (ethernet1/1)
 - Trust ゾーン:内部ネットワーク側(ethernet1/2)
- PA Firewall 内部の仮想ルーターには、Untrust ゾーンと Trust ゾーンのサブネット間ルーティングに加えて、イン ターネットへのデフォルトルートを設定します。
- インターネット方向のパケットは、送信元 IP アドレスを ethernet1/1 に設定された IP アドレスにアドレス変換 (NAT)して送出することにします。
- クライアント PC の DNS クエリ先は、内部 DNS(Windows Server 2012 R2)を指定しています。
- クライアント PC は、Windows ドメイン: acme.com に参加しています。

- 3. 初期設定
- 3.1. マネージメント IP の設定

マネージメントインターフェイスのデフォルト IP アドレスは、「192.168.1.1/24」(ハードウェアの場合)です。 (仮想マシンの場合は、DHCP がデフォルトです。)

そのまま利用することもできますが、本ガイドでは、以下のステップでネットワーク構成通りに変更します。

3.1.1. コンソール接続

コンソールポートに、PC の COM ポート・シリアルケーブルを接続します。

COM ポートの設定: Bits per sec: 9600 Data bits: 8 Parity: none Stop bits: 1 Flow control: none

例) PA-3050



3.1.2. CLI

マネージメントインターフェイスの IP アドレスを 192.168.55.11/24、デフォルトゲートウェイを 192.168.55.2 に設定します。

コンソール接続した PC のターミナル画面で、以下の赤文字部分を設定してください。

login: admin Password: admin

admin@PA-VM> configure

Entering configuration mode [edit]

admin@PA-VM# set deviceconfig system type static

admin@PA-VM#

admin@PA-VM# set deviceconfig system ip-address 192.168.55.11 netmask 255.255.255.0 default-gateway 192.168.55.2

admin@PA-VM# commit

Commit job 9 is in progress. Use Ctrl+C to return to command prompt75%98%......100% Configuration committed successfully

[edit] admin@PA-VM#

- 3.2. WebUI へのアクセス
- マネージメントインターフェイスが接続されたネットワーク上のコンソール用 PC から、ブラウザで https://192.168.55.11 ヘアクセスします。
- (2) 証明書の警告がでますが、そのままアクセスしてください。
- (3) 認証画面が出ますので、「ユーザ名:admin、パスワード:admin」を入力し、「Log In」ボタンを押します。

.,,//	paloalto	
Username	admin	
Password	•••••	
[Log In	

(4) Admin アカウントのパスワードをデフォルトのまま利用していることに関する警告がでます。「OK」を押します。



(5) Welcome 画面が出ます。「Close」をクリックします。

We	come	0					
	0						
	Welcome to PAN-OS 8.0!						
	This release includes many new features that enhance the threat prevention capabilities of the platform, provide improved visibility, and streamline your security management workflow including:						
	 Credential phishing prevention - User credential detection to prevent users from submitting corporate credentials to potentially untrusted sites. 						
	 Policy-based Multi-Factor Authentication (MFA) - Enable MFA at the network layer to protect sensitive resources and limit an adversary's ability to use compromised credentials or endpoints to move throughout the network. 						
	 Panorama logging enhancements to accelerate log queries and reports, support for Traps logs, and improved log collection on the Panorama virtual appliance. 						
	 VM-Series firewall performance enhancements and expanded model line. 						
	 Command-and-Control (C2) signature technology to automatically generate and deliver more powerful, pattern-based C2 sionatures with antivirus updates. 						
	 AWS CloudWatch integration - Publish VM-Series firewall metrics to monitor resource usage and set alarms on AWS CloudWatch. 						
	 Admin-level commit and revert for granularity in committing and reverting configuration changes. 						
	 Traffic inspection in cleartext tunnel protocol - GRE, non-encrypted IPSec, or GTP-U. 						
	 Selective log forwarding based on log attributes and action-oriented log forwarding using HTTP. 						
	 Panorama VMware NSX plugin to manage all security configurations for the VM-Series NSX integration. 						
	Refer to the PAN-OS 8.0 New Features Guide for a complete list of the new features and instructions on how to use them and the Do not show again						
		_					
	Cos	ie					

(6) ダッシュボード画面が表示されます。 以降、日本語のスクリーンショットを使っているので、日本語へ切り替えます。 右下にある、「Language」をクリックします。

🚚 paloalto												
	NETWORKS [®]	Dashboard A	CC		Monitor	Policies	Objects	Network	Device	🛎 Comr	mit 🎳 😡 Coi	nfig - 🦳 Search
		Layout: 3 Columns 🗸		🔡 Widge	ets – Last u	pdated: 1	6:13:46				5 mins	🔻 😋 🔞 Help
	General Information	S ×		Logged li	n Admins			S ×	Config Logs			S ×
	Device Name	PA-VM		Admin	From	Client	Session Start	Idle For	Command	Path	Admin	Time
	MGT IP Address	192.168.55.10		admin	192.168.55.1	Web	02/01 16:03:11	00:00:00s	commit		admin	02/01
	MGT Netmask	255.255.255.0		admin	192.168.55.1	CLI	02/01 15:30:18	00:06:23s	cot	dovicecentia	admin	15:35:35
	MGT Default Gateway	192.168.55.254							Set	system	dullilli	15:35:29
	MGT IPv6 Address	unknown	J.	Data Log	S			S 🛛	commit		admin	02/01
	MGT IPv6 Link Local Address	V6 Link Local Address fe80::20c:29ff:fee6:dd02/64			No data available.							15:30:31
	MGT IPv6 Default Gateway		II.	System Loas 🖸 🛪				S ×	Locks			S 🛛
	MGT MAC Address	00:0c:29:e6:dd:02	I.	Decerie				Time	No locks found			
	Model	PA-VM		Idan of a	Group-Mappin	g_001 fail	ad to connact	02/01				
	Serial #	015351000006989		to serve	r 192.168.45.6	5:389: En	ror: Failed to	16:13:38	ACC Risk Facto	r (Last 60 minutes)		S 🛛
	CPU ID	ESX:E9060900FFFBAB1F		connect	to 45 65(192 168	160 45 65):200Error:			No data found			
	UUID 564DD15A-3F43-55C7-E81D- 031C5FE6DD02		•	Failed to connect to 192.168.45.65(192.168.45.65):389 192.168.45.65(192.168.45.65):389								
	VM License	VM-50		ldap cfg	Group-Mappin	g-001 fail	ed to connect	02/01				
	VM Mode	VMWare ESXi		to serve	r 192.168.45.6	5:389: Er	ror: Failed to	16:12:18				
	Software Version	8.0.6		192.168	.45.65(192.168	3.45.65):3	89Error:					
	GlobalProtect Agent	4.0.4		Failed to	connect to	AE 651.2	200					
adimin Logout Last Login Time: 02/01/2018 15:30:18								👼 Task: Language				

(7) 表示された画面のプルダウンメニューから、日本語を選択して、「OK」ボタンを押します。

Language Preferen	ce	0
Language	English	
	English	
	日本語	
	Español	-
	简体中文	
	Français	
	繁體中文	

(8) メッセージ画面が出ます。「今後は表示しない」にチェックを入れて、「閉じる」をクリックします。

歓	迎の言葉	0
	•	
	PAN-OS 8.0 へようこそ!	
	This release includes many new features that enhance the threat prevention capabilities of the platform, provide improved visibility, and streamline your security management workflow including:	
	 Credential phishing prevention - User credential detection to prevent users from submitting corporate credentials to potentially untrusted sites. 	
	 Policy-based Multi-Factor Authentication (MFA) - Enable MFA at the network layer to protect sensitive resources and limit an adversary's ability to use compromised credentials or endpoints to move throughout the network. 	
	 Panorama logging enhancements to accelerate log queries and reports, support for Traps logs, and improved log collection on the Panorama virtual appliance. 	
	 VM-Series firewall performance enhancements and expanded model line. 	· ·
	 Command-and-Control (C2) signature technology to automatically generate and deliver more powerful, pattern-based C2 signatures with antivirus updates. 	
	 AWS CloudWatch integration - Publish VM-Series firewall metrics to monitor resource usage and set alarms on AWS CloudWatch. 	
	 コミットおよび取り消し設定の粒度の管理者レベルのコミットおよび取り消しが変更されました。 	
	 Traffic inspection in cleartext tunnel protocol - GRE, non-encrypted IPSec, or GTP-U. 	
	 Selective log forwarding based on log attributes and action-oriented log forwarding using HTTP. 	
	 Panorama VMware NSX plugin to manage all security configurations for the VM-Series NSX integration. 	
	◇ 今後は表示しない	
		వ

3.3. DNSとNTPの設定

PA Firewall が参照する DNS サーバーと NTP サーバーの設定を行います。

(1) a) $\lceil \text{Device}
ightarrow$ b) $\lceil tz_{y}
vert P_{y}
vert^{2}
ightarrow$ c) $\lceil tz_{y}
vert - tz_{y}
vert$ d) $\stackrel{!}{x}$ P $r
vert^{2}
vert p_{y}
vert^{2}
vert$ c) $\lceil tz_{y}
vert^{2}
vert$ c) \rceil d) $\stackrel{!}{x}$ P $r
vert^{2}
vert^{2}
vert^{2}$ c) $\lvert tz_{y}
vert^{2}
vert^{2}
vert^{2}
vert^{2}$ c) $\lvert tz_{y}
vert^{2}
vert^{2}
vert^{2}
vert^{2}$ c) $\lvert tz_{y}
vert^{2}
vert^{2}
vert^{2}
vert^{2}
vert^{2}
vert^{2}
vert^{2}
vert^{2}$ c) $\lvert tz_{y}
vert^{2}
v$



(2) a)「プライマリ/セカンダリ DNS サーバー」に、利用する DNS サーバーの IP アドレスを入力しまします。 本ガイドでは、プライマリ DNS に 192.168.55.2、セカンダリ DNS に 4.2.2.2 を指定しています。

次に、b)「NTP」タブをクリックします。

サービス	Q
サービス NTP b)	
DNS ● サー	バー 🔿 DNS プロキシ オプジェクト
プライマリ DNS サーバー	192.168.55.2 a)
セカンダリ DNS サーバー	4.2.2.2
更新サーバー	updates.paloaltonetworks.com
(✔ 更新サーバー ID の確認
Proxy Server	
サーバー	
ポート	[1 - 65535]
ユーザー	
パスワード	
再入力 パスワード	

(3) a)「NTP サーバー アドレス」に、利用する NTP サーバー(例:ntp.nict.jp)を入力します。 b)「OK」をクリックします。

サ	ーピス					0
Ŧ	ービス NTP					
Г	ブライマリ NTP サーバー			セカンダリ NTP サーバー		
	NTP サーバー アドレス	ntp.nict.jp	a)	NTP サーバー アドレス		
	認証タイプ	なし	~	認証タイプ	なし	~
					b) ок	キャンセル

(4) タイムゾーンを日本に変更します。 a)「Device」 → b)「セットアップ」 → c)「管理」 → 「一般設定」の d) $\stackrel{\circ}{\stackrel{\circ}{\xrightarrow}}$ アイコンをクリックします。

,,,,,, paloalto		100						•		
NETWORKS [®]	Dashboard	ACC	Monitor	Policies	Objects	Network	Device			
						L L		J		
 ○ セットアップ b) 	C) 管理 操作	サービス	インターフ	エイス テレ	レメトリー	コンテンツID	WildFire	セッション	HSM	
№ 設定監査	一般設定						*	Paliorama 設定		
				ホスト名	PA-VM			_		
◎ 管理者ロール				5823					Panorama	
😢 認証プロファイル									Parlorania	
2 認証シーケンス				ログイン パナー				Panorama		
■ ユーザー ID		ログ	イン パナーの確認	8を管理者に強制					Panorama (C	
VM 情報ソース			SSL/TLS サービ	ス プロファイル						
▼ 🚰 証明書の管理				タイト ゾーン	LIS/Pacific					
፼ 証明書					objrucine					
🐖 証明書プロファイル				表示言語	en					
Note Contract Contra				時間	Wed Feb 28 22	2:19:10 PST 2018		バナーとメッ	セージ	
🔒 SSL/TLS サービス プロフォ			5	「バイス稼働場所			E			
SCEP										
🗧 🔒 SSL 復号化例外	² SSL 復号化例外 二ミット ロッソの日期実施									
◎ 応答ページ	証明書有効期限チェック									
目ログ設定	ハイパーバイザによって割り当てられた MAC アドレスの使用 🛛 🗸									
▼ 4 サーバー プロファイル	GTP Security									
SNMP トラップ				on becany						
Suctors .										

(5) a)タイムゾーンで、「Asia/Tokyo」を選択し、b)「OK」をクリックします。

一般設定	0
ホスト名	PA-VM
ドメイン	
	DHCP サーバー提供のホスト名を受け入れる
	□ DHCP サーバー提供のドメインを受け入れる
ログイン バナー	
	□ ログイン パナーの確認を管理者に強制
SSL/TLS サービス プロファ	None
タイム ゾーン	Asia/Tokyo a)
表示言語	en 💌
日付	2018/02/28 💌
時間	22:19:10 💌
緯度	
経度	
	□ コミット ロックの自動実施
	証明書有効期限チェック
	✓ ハイパーバイザによって割り当てられた MAC アドレスの
	使用
	GTP Security
	b) OK キャンセル

3.4. 設定のコミット

実施した設定を反映するためには、コミットが必要です。

(1) 画面右上の「コミット」をクリックします。

naloalto										
NETWORKS®	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	📥 コミット	💣 🛯 🧶 Config 👻 🔍 💆	家
									S 0/	ヘルプ

(2)「Commit すべての変更」にチェックが入っていることを確認して、「コミット」をクリックします。



3.5. ライセンス投入

3.5.1. サポートライセンス

サポートライセンスの投入ステップです。

サポートライセンスを購入することで、OSのダウンロードや基本保守が受けられるようになります。(必須)

(1) a)「Device」→ b)「サポート」で表示された画面の「サポート」の下の c)「認証コードを使用したサポートのアクティベーション」をクリックします。

paloalto	Dashboard ACC Monitor Policies Objects Network Device	🍐 コミット 🧉 🔯 Config 🕶 🔍 検索
		ら のヘルプ
INETION	サポート リンク	
 TACACS+ LDAP Kerberos SAMLアイデンティティ 	連絡生 Click the contact lick at doht 認証コードを使用したサポートのアクティペーション C) COntact Us サポート ページ デバイスの登録	
▼ □ ローカル ユーザー データ^	実働アラート テクニカル サポート ファイル	
S ユーザー S ユーザー グループ	、 実稼働アラートなし テクニカル サポート ファイルの生成	
 	Stats Dump ファイル	
GlobalProtect クライアント ダイナミック更新	アプリケーションおよび脅威アラート Stats Dump ファイルの生成	
● サポート b)	アプリケーションおよび脅威アラートなし コアファイル コアファイルなし	

(2) 認証コード(ライセンス証書に記載された Auth Code)を入力して、「OK」をクリックします。



(3) 有効期限を確認します。



3.5.2. 機能ライセンス

各機能のライセンス投入ステップです。

機能ライセンスを投入することで、各セキュリティ機能が有効になります。

(1) a)「Device」→ b)「ライセンス」→ c)「認証コードを使用した機能のアクティベーション」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	🏝 コミット 🤷 🍃 Conlig 🗝 🔍 検索
								S ()~//7
In Netflow RADIUS RADIUS RADIUS TACACS+ LDAP Kerberos SAML アイデンティティ マルチ ファクター認証 マルチ ファクター認証 マーカル ユーザー データ・ Sユーザー グループ スケジュール設定されたロ ペリント ウェア GlobalProtect クライアント ゲィキング 美数 マイセンス D) マパート マスターキーおよび診断	ライセンス管理 ライセンス サーバ 駆逐コードを使用 ライセンス キーの VM の非アクティン VM キャパシティの	ーからライヤン した機能のアク 手動アップロー プ化 Dアップグレー	ンス キーを取得 フティペーション ード	C)				

(2) 認証コード(ライセンス証書に記載された Auth Code)を入力して、「OK」をクリックします。



- (3) (仮想マシンの場合、自動的にリブートされます。)
- (4) WebUIに再ログインし、購入した機能が有効になっているか、またその有効期限などを確認します。

例:脅威防御



3.6. シグネチャのダウンロードとインストール

アプリケーション識別やアンチウイルス等の各種セキュリティ機能が利用するシグネチャのダウンロードを行います。 更に、それらのダウンロードとインストールが自動的に行われるように設定します。

3.6.1. ダイナミック更新

アプリケーション/脆弱性防御/スパイウェア/アンチウイルスのシグネチャのダウンロードとインストールを行います。

(1) a) 「Device」 \rightarrow b) 「ダイナミック更新」 \rightarrow c) 「今すぐチェック」をクリックします。

🚚 paloalto

NETWORKS®	Dashboard	ACC	Monitor	Policies	Objects	Network	Device		ě :	コミット 💣	🛵 Config 👻 🔍	検索
											S 🛛)ヘルプ
💀 OCSP レスポンダ											2 個の項目s	- x
 B SSL/TLS サービス プロフェ 国 SCEP B SSL 復号化例外 	パージョン ファ	イル名	機能	9-	イプサイ	「ズ リリースE	3	ダウンロー ド済み	現在インス トール済み	アクション	ドキュメント	
◎ 応答ページ	▽ GlobalProtect ク	ライアントレスヽ	/PN 最終:	チェック: never	スケジュー	l: None						
 ■ ログ設定 ▶ ゆ サーバー プロファイル ▶ 回 ローカル ユーザー データベー 	▽ GlobalProtect デ	ータ ファイル	スケジュ	– אי: None								
■ スケジュール設定されたログ(● いっとウェマ												
② ワイナミック更新 D) ③ ダイナミック更新 D) ④ ダイナミック更新 D) ● サポート ● マスターキーおよび診断	<mark>C)</mark> こ 今すぐチェック	🛓 アップロー	ド 📘 ファイルカ	からインストー	IL							

(2) 以下画面のように、ダウンロードできるシグネチャの一覧が表示されます。

最新の「アプリケーションおよび脅威」シグネチャの、アクション列の「ダウンロード」をクリックします。

NETWORKS.	Dashbo	ard Acc Monitor	Folicies Object	s Netwo	лк и	evice				
										S @~//
😺 セットアップ	۹,									17 個の項目s 🔿 (
□ 高可用性 □ 設定監査	バージョン	ファイル名	機能	タイプ	サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント
パスワード プロファイル	▽ アプリケーミ	ションおよび脅威 最終チェック	: 2018/02/07 22:24:37 PST	スケジュール	: Every We	dnesday at 01:02 (Downle	oad only)			
S 管理者	777-4494	panupy2-all-contents-777-4484	Apps Threats	Full	44 MB	2018/02/06 21:20:15 PST		[ダウンロード	00-7 /-b
◎ 管理者ロール	770-4445	panupy2-all-contents-770-4445	Apps, Threats	Full	36 MB	2018/01/23 20:50:00 PST		L	ダウンロード	111-7 /- k
28認証プロファイル	771-4450	panupy2-all-contents-771-4450	Apps, Threats	Full	36 MB	2018/01/26 10:56:17 PST			ダウンロード	
※ 認証シーケンス	775-4476	panupy2-all-contents-775-4476	Apps, Threats	Full	36 MB	2018/02/05 15:44:22 PST			ダウンロード	UU-2 / N
2 104 (##8) (_ 7	773-4465	panupy2-all-contents-773-4465	Apps, Threats	Full	36 MB	2018/02/01 21:13:44 PST			ダウンロード	リリース ノート
「「日報ノーへ」	772-4461	panupv2-all-contents-772-4461	Apps, Threats	Full	36 MB	2018/01/31 14:55:25 PST			ダウンロード	リリース ノート
	766-4424	panupy2-all-contents-766-4424	Apps, Threats	Full	36 MB	2018/01/11 20:18:47 PST			ダウンロード	リリースノート
■ 証明書プロファイル	776-4482	panupv2-all-contents-776-4482	Apps, Threats	Full	36 MB	2018/02/06 12:57:29 PST			ダウンロード	リリース ノート
GCSP レスポンダ	768-4429	panupv2-all-contents-768-4429	Apps, Threats	Full	36 MB	2018/01/16 13:18:31 PST			ダウンロード	リリース ノート
🔓 SSL/TLS サービス プロファイ	774-4467	panupv2-all-contents-774-4467	Apps, Threats	Full	36 MB	2018/02/02 06:15:26 PST			ダウンロード	リリース ノート
SCEP 1	769-4439	panupv2-all-contents-769-4439	Apps, Threats	Full	36 MB	2018/01/17 20:27:14 PST			ダウンロード	リリース ノート
🔒 SSL 復号化例外	765-4419	panupv2-all-contents-765-4419	Apps, Threats	Full	36 MB	2018/01/09 10:40:20 PST			ダウンロード	リリース ノート
◎ 応答ページ	778-4489	panupv2-all-contents-778-4489	Apps, Threats	Full	44 MB	2018/02/07 20:22:22 PST			ダウンロード	リリース ノート
目ログ設定	767-4427	panupv2-all-contents-767-4427	Apps, Threats	Full	36 MB	2018/01/12 15:58:22 PST			ダウンロード	リリース ノート
リーパー プロファイル ローカル ユーザー データベース	⊳ GlobalProt	ect クライアントレス VPN 最佳	チェック: 2018/02/07 22:2	4:43 PST スク	ァジュール:	None				
スケジュール設定されたログのエ のトリストウェス	⊽ GlobalProt	ect データ ファイル スケシ	ュール: None							
ClobalProtect クライアント										
School (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	⊽ WildFire	最終チェック: 2018/02/07 22:24	:41 PST スケジュール: N	lone						
ヘフィセンス ジサポート 日 マスター キーおよび診断	216490-218887	panupv2-all-wildfire-216490-218887	PAN-OS 7.1 and later	Full	9 MB	2018/02/07 22:14:56 PST			ダウンロード	リリース ノート

(3) ダウンロードが開始されます。完了するまで待ちます。

アプリケーションおよび脅威 のダウンロード	0
操作 ダウンロード	
状態 アクティブ	
結果 保留	
進捗 99%	
詳細	
警告	
	閉じる

(4) アクション列の「インストール」をクリックします。

		Dashboar	d ACC	Monitor	Policies Obj	iects Netwo	ork C	levice			*	コミット 🧉 阔 Config 🕶 🔍 検索
												5 ⑦ヘルプ
🨺 t	ットアップ	٩										17 個の項目s 🗙
「二高」。	可用性 定監査	バージョン	ファイル名		機能	タイプ	サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント
۲۲ 🦻 🖉	スワード プロファイル 四本	▽ アプリケーショ	ョンおよび脅威	最終チェック	2018/02/07 22:25:22 P	ST スケジュール:	Every We	ednesday at 01:02 (Downl	oad only)	_		
1	理者ロール	777-4484	panupv2-all-conte	nts-777-4484	アプリケーション, Th	nreats Full	44 MB	2018/02/06 21:20:15 PST	~	L	インストール ポリシーのプレビュ	リリース ノート 🗵
188 1921 - 1922 - 192 - 192 - 1922 - 192 - 1922 - 1922 - 1922 - 1922 - 1922 - 1922 - 1922 - 1922 - 192 - 1922 - 19	証プロファイル IFFシーケンス	770-4445	panupv2-all-conte	nts-770-4445	Apps, Threats	Full	36 MB	2018/01/23 20:50:00 PST			ダウンロード	リリース ノート

(5)「インストールの続行」をクリックします。 アプリケーションおよび脅威のインストール

アフリケーションねよい育成の1 ノストール 🕔									
 コンテンツ更新での新しいアプリケーションの無効 化 									
	インストールの続行	キャンセル							

(6) インストールが完了すると、a)現在インストール済み列にチェックが入った状態になります。 もう一度、b)「今すぐチェック」をクリックします。

	Dashboa	ard ACC Monitor	Policies Object	s Netwo	ork Device				🛎 コミット 🧉 👰 Config 🕶 🤇 検索
									ち のヘルプ
闷 セットアップ	۹.								17 個の項目s 🗎
高可用性	バージョン	ファイル名	機能	タイプ	サイズ リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント
>2 設定監査 ↓↓ パスワード プロファイル	-								
会 管理者	▽ アプリケーシ	/ヨンおよび骨底 最終チェック	: 2018/02/07 22:25:22 PST	スケジュール	: Every Wednesday at 01:02 (Downlo	oad only)		9	
20管理者ロール	777-4484	panupv2-all-contents-777-4484	Apps, Threats	Full	44 MB 2018/02/06 21:20:15 PST	~	:		リリース ノート 🗵
総認証プロファイル	770-4445	panupv2-all-contents-770-4445	Apps, Threats	Full	36 MB 2018/01/23 20:50:00 PST		••••••	ダウンロード	リリース ノート
5部 認証シーケンス	771-4450	panupv2-all-contents-771-4450	Apps, Threats	Full	36 MB 2018/01/26 10:56:17 PST			ダウンロード	リリース ノート
ID ユーザー ID	775-4476	panupv2-all-contents-775-4476	Apps, Threats	Full	36 MB 2018/02/05 15:44:22 PST			ダウンロード	リリース ノート
WM 情報ソース	773-4465	panupv2-all-contents-773-4465	Apps, Threats	Full	36 MB 2018/02/01 21:13:44 PST			ダウンロード	リリース ノート
▼ 🚰 証明書の管理	772-4461	panupv2-all-contents-772-4461	Apps, Threats	Full	36 MB 2018/01/31 14:55:25 PST			ダウンロード	リリース ノート
■ 証明書	766-4424	panupv2-all-contents-766-4424	Apps, Threats	Full	36 MB 2018/01/11 20:18:47 PST			ダウンロード	リリース ノート
🔁 証明書プロファイル	776-4482	panupv2-all-contents-776-4482	Apps, Threats	Full	36 MB 2018/02/06 12:57:29 PST			ダウンロード	リリース ノート
OCSP レスポンダ	768-4429	panupv2-all-contents-768-4429	Apps, Threats	Full	36 MB 2018/01/16 13:18:31 PST			ダウンロード	リリース ノート
👸 SSL/TLS サービス プロファイ	774-4467	panupv2-all-contents-774-4467	Apps, Threats	Full	36 MB 2018/02/02 06:15:26 PST			ダウンロード	リリース ノート
I SCEP	769-4439	panupv2-all-contents-769-4439	Apps, Threats	Full	36 MB 2018/01/17 20:27:14 PST			ダウンロード	リリース ノート
SSL 復号化例外	765-4419	panupv2-all-contents-765-4419	Apps, Threats	Full	36 MB 2018/01/09 10:40:20 PST			ダウンロード	リリース ノート
	778-4489	panupv2-all-contents-778-4489	Apps, Threats	Full	44 MB 2018/02/07 20:22:22 PST			ダウンロード	リリース ノート
● ログ設定	767-4427	panupv2-all-contents-767-4427	Apps, Threats	Full	36 MB 2018/01/12 15:58:22 PST			ダウンロード	リリース ノート
▶ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	▷ GlobalProte	ect クライアントレス VPN 最	修チェック: 2018/02/07 22:24	:43 PST スク	アジュール: None				
スケジュール設定されたログのエ	,								
☜ソフトウェア		act データ ファイル スケシ	ノュール: None						
😢 GlobalProtect クライアント									
ダイナミック更新 く ライヤンス	⊽ WildFire	最終チェック: 2018/02/07 22:2	4:41 PST スケジュール: N	one					
ジサポート	216490-218887	panupv2-all-wildfire-216490-21888	PAN-OS 7.1 and later	Full	9 MB 2018/02/07 22:14:56 PST			ダウンロード	リリース ノート
🔒 マスター キーおよび診断	b)								
	ら 今すぐチェ	ック 🛓 アップロード 📘 ファイノ	しからインストール						

(7) 「アンチウイルス」シグネチャのダウンロードが可能になります。 最新のシグネチャの、アクション列の「ダウンロード」をクリックします。

	Dashboa	ard ACC Monitor	Policies Object	ts Netwo	ork D	evice			2	コミット 🧉 陽 Config 🕶 🔍 検索
										5 のヘルプ
🖓 セットアップ	۹.									21 個の項目s 🔿 🗙
➡高可用性 ➡ 設定監査	パージョン	ファイル名	機能	タイプ	サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント
<⊓パスワード プロファイル	▽ アンチウイル	ス 最終チェック: 2018/02/07	22:28:30 PST スケジュー	JL: None				_		
20 日本10 20 管理来ロール	2514-3010	panup-all-antivirus-2514-3010		Full	84 MB	2018/02/07 04:04:56 PST			ダウンロード	リリース ノート
12日日 ル	2513-3009	panup-all-antivirus-2513-3009		Full	84 MB	2018/02/06 04:01:42 PST			ダウンロード	リリース ノート
28 認証シーケンス	2511-3005	panup-all-antivirus-2511-3005		Full	85 MB	2018/02/03 04:04:44 PST			ダウンロード	リリース ノート
10 ユーザー ID	2512-3007	panup-all-antivirus-2512-3007		Full	84 MB	2018/02/04 18:29:38 PST			ダウンロード	リリース ノート
WM 情報ソース	▽ アプリケーシ	マヨンおよび脅威 最終チェック	: 2018/02/07 22:28:28 PST	スケジュール	: Every We	dnesday at 01:02 (Downl	oad only)			
▼ 4回 証明書の管理	777-4484	panupv2-all-contents-777-4484	Apps, Threats	Full	44 MB	2018/02/06 21:20:15 PST	~	~		リリース ノート 🛛 🕱
₩ 証明書	770-4445	panupv2-all-contents-770-4445	Apps, Threats	Full	36 MB	2018/01/23 20:50:00 PST			ダウンロード	リリース ノート
GCSP レスポンダ	771-4450	panupv2-all-contents-771-4450	Apps, Threats	Full	36 MB	2018/01/26 10:56:17 PST			ダウンロード	リリース ノート
B SSL/TLS サービス プロファイ	775-4476	panupv2-all-contents-775-4476	Apps, Threats	Full	36 MB	2018/02/05 15:44:22 PST			ダウンロード	リリース ノート
SCEP	773-4465	panupv2-all-contents-773-4465	Apps, Threats	Full	36 MB	2018/02/01 21:13:44 PST			ダウンロード	リリース ノート
🔒 SSL 復号化例外	772-4461	panupv2-all-contents-772-4461	Apps, Threats	Full	36 MB	2018/01/31 14:55:25 PST			ダウンロード	リリース ノート
💫 応答ページ	766-4424	panupv2-all-contents-766-4424	Apps, Threats	Full	36 MB	2018/01/11 20:18:47 PST			ダウンロード	リリース ノート
📑 ログ設定	776-4482	panupv2-all-contents-776-4482	Apps, Threats	Full	36 MB	2018/02/06 12:57:29 PST			ダウンロード	リリース ノート
▶ 👘 サーバー プロファイル	768-4429	panupv2-all-contents-768-4429	Apps, Threats	Full	36 MB	2018/01/16 13:18:31 PST			ダウンロード	リリース ノート
▶ 🛄 ローカル ユーザー データベース	774-4467	panupv2-all-contents-774-4467	Apps, Threats	Full	36 MB	2018/02/02 06:15:26 PST			ダウンロード	リリース ノート
スケジュール設定されたログのコ	769-4439	panupv2-all-contents-769-4439	Apps, Threats	Full	36 MB	2018/01/17 20:27:14 PST			ダウンロード	リリース ノート
◎ ソフトウェア	765-4419	panupv2-all-contents-765-4419	Apps, Threats	Full	36 MB	2018/01/09 10:40:20 PST			ダウンロード	リリース ノート
SolobalProtect クライアント	778-4489	panupv2-all-contents-778-4489	Apps, Threats	Full	44 MB	2018/02/07 20:22:22 PST			ダウンロード	リリース ノート
2. ダイナミック史新	767-4427	panupv2-all-contents-767-4427	Apps, Threats	Full	36 MB	2018/01/12 15:58:22 PST			ダウンロード	リリース ノート
<> ライセンス ⇒ サポート	⊳ GlobalProte	ect クライアントレス VPN 最終	冬チェック: 2018/02/07 22:2	8:34 PST ス	ケジュール:	None				
🔒 マスター キーおよび診断	⊽ GlobalProte	act データ ファイル スケシ	ュール: None							
	⊽ WildFire	最終チェック: 2018/02/07 22:20	8:33 PST スケジュール: M	lone						
	216490-218887	panupv2-all-wildfire-216490-218887	PAN-OS 7.1 and later	Full	9 MB	2018/02/07 22:14:56 PST			ダウンロード	リリース ノート
	の合すぐチェ	ック ・ アップロード 📑 ファイル	からインストール							

(8) アクション列の「インストール」をクリックします。

	Dashboa	rd ACC	Monitor	Policies	Objects	Netwo	ork D	evice			\$	コミット 💣 阔) Config - 鸟検	索
													S @^	ルプ
しまた、 しゃういう しょういう しょう しょう しょう しょう しょう しょう しょう しょ しょういう しょう しょう しょう しょう しょう しょう しょう しょう しょう しょ	٩												21 個の項目s 📑	• ×
□ 高可用性 □ 設定監査	パージョン	ファイル名		機能		タイプ	サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	1	ドキュメント	
《 パスワード プロファイル 《 MTR#	▽ アンチウイル	ス 最終チェック:	: 2018/02/07 22:	:29:40 PST	スケジュール:	None				_		_		
る 言理者	2514-3010	panup-all-antivirus-251	4-3010			Full	84 MB	2018/02/07 04:04:56 PST	~		インストール	1	ノリース ノート	×
122 認証プロファイル	2513-3009	panup-all-antivirus-251	3-3009			Full	84 MB	2018/02/06 04:01:42 PST			ダウンロード	1	リリース ノート	
1 認証シーケンス	2511-3005	panup-all-antivirus-251	1-3005			Full	85 MB	2018/02/03 04:04:44 PST			ダウンロード	1	ノリース ノート	
III ユーザー ID	2512-3007	panup-all-antivirus-251	2-3007			Full	84 MB	2018/02/04 18:29:38 PST			ダウンロード	1	リリース ノート	
WM 情報ソース	- アプリケーシ	コンお上が身成	暴怒チェック・つ	018/02/07 22-	28-28 PCT 7	はたジュール。	Even We	dneeday at 01:02 (Downly	(vlao beo					

(9) インストールが完了すると、a)「現在インストール済み」列にチェックが入った状態になります。

シグネチャの自動インストールの設定を行います。 b)「スケジュール: None」をクリックします。

paloalto	Dashboa	rd ACC	Monitor	Policies	Objects	Netw	ork D	evice			đ	造 그 ミット 🧉 ಢ Config 🕶 🔍	検索
												S 0	ヘルプ
😡 セットアップ	٩											21 個の項目s	⇒ ×
□● 高可用性 □>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	パージョン	ファイル名		機能		タイプ	サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント	
パスワード プロファイル	▽ アンチウイル	ス 最終チェッ	7: 2018/02/07 2	2:29:40 PST	スケジュール:	None	D)						
る 管理者	2514-3010	panup-all-antivirus-	2514-3010			Pull	84 MB	2018/02/07 04:04:56 PST	¥	 a) 		リリース ノート	×
	2513-3009	panup-all-antivirus-	2513-3009			Full	84 MB	2018/02/06 04:01:42 PST			ダウンロード	リリース ノート	
2 認証シーケンス	2511-3005	panup-all-antivirus-	2511-3005			Full	85 MB	2018/02/03 04:04:44 PST			ダウンロード	リリース ノート	
ID ユーザー ID	2512-3007	panup-all-antivirus-	2512-3007			Full	84 MB	2018/02/04 18:29:38 PST			ダウンロード	リリース ノート	
VM 情報ソース		- s. des L. enfaltente											

(10) 表示された画面で、アンチウイルスシグネチャの更新スケジュールを以下のように設定します。

アンチウイル	スの更新に	マケジュール 💿	
	繰り返し	每時	a)毎時
分((過去 1 時間)	0	
	アクション	download-and-install	b) download-and-install
UI	きい値 (時間)	[1 - 120] 実行するすべてのアクションについて、コンテンツは少なくともこれ以 上古い必要があります	
		C) OK キャンセル	

(11) 同様の方法で、アプリケーションと脅威シグネチャの更新スケジュールも以下のように設定します。

アプリケーシ	ョンと脅闘	或の更新スケジュール 💿	
	繰り返し	毎時	a)毎時
分 (過去 1 時間)	0	
	アクション	download-and-install	b) download-and-instal
		□ コンテンツ更新での新しいアプリケーションの無効化	
61	きい値 (時間)	[1 - 120]	
		実行するすべてのアクションについて、コンテンツは少なくともこれ以 上古い必要があります	
		C) () キャンセル	

(12) 同様の方法で、Wildfire シグネチャの更新スケジュールも以下のように設定します。

WildFire の更新	スケジュ・	- <i>ル</i>	0	
	繰り返し	毎分	V	a)毎分
	アクション	download-and-install	•	b) download-and-install
		с) ок	キャンセル	

3.6.2. URL フィルタリングのシグネチャ

URL フィルタリングのシグネチャは、上記の「ダイナミック更新」とは異なり、「ライセンス」画面でダウンロードします。

(1) a)「Device」 \rightarrow b)「ライセンス」 \rightarrow PAN-DB URL Filtering 下の c)「今すぐダウンロード」をクリックします。



(2) 警告が出ますが、「はい」をクリックします。



(3) ダウンロードする領域を選びます。本ガイドでは a)「Japan」を選択しています。b)「OK」をクリックします。



- (4) 「ダウンロードが成功しました」というメッセージが出たら、「閉じる」をクリックします。
- (5) 以下のように、「Finished Successfully」となれば完了です。



3.7. OS アップグレード

PAN-OS8.1.0 へのアップグレードを行います。 インターネット経由で必要な OS をダウンロードしてインストールします。

(1) a)「Device」→ b)「ソフトウェア」をクリックします。
 初回だけ「操作失敗」のエラーが出ますが、c)「閉じる」をクリックします。

paloalto	Dashboard	ACC Mon	itor Policies	Objects Net	work Device		参コミット 着	🔞 Config 🔻 🔍 検索
					a)			ら のヘルプ
TACACS+	٩							0個の項目s → Ӿ
	パージョン	サイズ	リリース日	使用可能	現在インストール済 み	アクション		
マルチファクター認証 マルチファクター認証 マローカル ユーザー データ^			操作失敗					
8 ユーザー	4		No update informa	tion available				
 シフトウェア D) GlobalProtect クライアント ダイナミック更新 				閉じる	(C)			
ペライセンス ジサポート クファター モーヤトバ診断			-					
	⑤ 今すぐチェック	📥 アップロード						

(2) 「今すぐチェック」をクリックします。

	Dashboard	ACC	Monitor Policie	es Objects	Network Device		🏝 コミット 🧉 陽 Config 🕶 🔍 検索
							ର ଡିଏନ
TACACS+	٩						0 個の項目s 🏓 🕄
LDAP Kerberos	バージョン	サイズ	リリース日	使用可能	現在インスト- み	^{ール済} アクション	
 SAML アイデンティティ マルチ ファクター認証 マ □ ローカル ユーザー データッ シューザー シューザー グループ スケジュール設定された口 ひょ ソフトウェア GlobalProtect クライアント 							
 熱ダイナミック更新 ライセンス サポート マスター キーおよび診断 	G 今すぐチェック	<u>≟</u> アップロー	я				

(3) 現在リリースされている OS の一覧が表示されます。

a)「現在インストール済み」フィールドにチェックが入っているものが、現在の OS バージョン(本例では 8.0.7)です。

本ガイドでは、8.1.0 へのバージョンアップを行います。8.1.0 の行の b)「ダウンロード」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Netwo	rk Device		å =	コミット 省 🎑	Config 🕶	Q.検索
											9	@~//7
闷 セットアップ	۹.										89 個の項目	💵 🔿 🕽
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	バージョン	サイズ	リリース日		使用可能	3	現在インストール済み		アクション			
パスワード プロファイル	8.1.0	663 MB	2018/03/01	20:10:59					ダウンロード b)	リリース ノート		
5 管理者	8.0.8	431 MB	2018/02/11	09:42:06				••••••	977 XO - K	UU-7.7-P		
🐼 管理者ロール	8.0.7	431 MB	2017/12/28	10:26:05	Downloaded		~		再インストール	リリース ノート	a)	
88 認証プロファイル	8.0.6	431 MB	2017/11/13	22:44:23					ダウンロード	リリース ノート		

(4) ソフトウェアのダウンロードが開始されます。完了するまで待ちます。

ソフトウェ:	アのダウンロード	0
操作	ダウンロード	
状態	アクティブ	
結果	保留	
進捗	99%	
詳細	Successfully downloaded Preloading into software manager	
警告		
	閉じる	

(5) 「インストール」をクリックします。

paloalto	Dashboard	ACC	Monitor Poli	icies Objects	Network Device	e	🏝 コミット 🧉 闷 Co	nfig ▼ � 検索
								S @~//;
😡 セットアップ	۹.						89	個の項目s 🗦 🕽
□ 高可用性 □ 設定監査	パージョン	サイズ	リリース日	使用可能	現在インストール	済み アクション	_	
< パスワード プロファイル	8.1.0	663 MB	2018/03/01 20:10:	59 Downloaded		インストール	リリース ノート	×
🙎 管理者	8.0.8	431 MB	2018/02/11 09:42:	06		ダウンロード	リリース ノート	
😥 管理者ロール	8.0.7	431 MB	2017/12/28 10:26:	05 Downloaded	~	再インストール	リリース ノート	
認証プロファイル	8.0.6	431 MB	2017/11/13 22:44:	23		ダウンロード	リリース ノート	

(6) 以下のような警告が出ます。

ここまでの設定では、バックアップを要するほどの設定はしていませんので、「OK」をクリックします。



(7) インストールが開始されます。完了するまで待ちます。

ソフトウェアパ	ージョン 8.1.0 のインストール	0
操作 ソフ	トウェアのインストール	
状態 アク	ティブ	
結果 保留		
進捗	61%	
詳細		
警告		
		羽じる

(8) 再起動を促す画面が表示されますので、「OK」をクリックします。



(9) 再起動が行われます。(再起動するまでに5分程度かかります。)



- (10) 再起動後、PA Firewall の WebUI に再ログインします。
 - a)「Dashboard」 → 「一般的な情報」内の b)「ソフトウェアバージョン」が、インストールしたバージョンになっていることを確認します。

naloalto				_			
NETWORKS®	Dashboard ACC	Monitor Policies Objects Networ	k Device		🛎 コミット	💣 🛛 👰 Config	▼ 9.検索
	レ·(アウa): 3列 🔍 🗸	🔡 ウィジット - 最終更新: 17:28:13			5分	V	ら ③ヘルプ
一般的な情報	S ×	ログインしている管理者	S ×	設定ログ			S 🛛
デバイス名	PA-VM	管理者 送信者 クライアント セッション開始	アイドル状態	コマンド	パス	管理者	時間
MGT IP アドレス	192.168.55.11	admin 192.168.55.1 Web 03/24 17:28:29	00:00:00s	commit		admin	03/24 17:10:51
MGT ネットマスク	255.255.255.0			set	deviceconfig system	admin	03/24
MGT デフォルト ゲートウェイ	192.168.55.2	<u>テータログ</u>	S X				17:10:40
MGT IPv6 アドレス	unknown	使用可能データなし.		set	deviceconfig system	admin	03/24
MGT IPv6 リンク ローカル ア	fe80::20c:29ff:fe88:b63d/64			delete	deviceconfig system	admin	03/24
トレス		システム ログ	S X	delete	dns-setting dns-proxy-	damm	17:10:18
MGT IPV0 デフォルド ワード ウェイ		内容	時間		object		
MGT MAC アドレス	00:0c:29:88:b6:3d	Autocommit job succeeded	03/24 17:28:31	delete	deviceconfig system dns-setting dns-proxy-	admin	03/24 17:10:18
モデル	PA-VM	Dnsproxy object:mgmt-obj was enabled.	03/24		object		00/04
シリアル番号	015351000008994		17:28:29	commit		admin	17:07:06
CPU ID	ESX:E9060900FFFBAB1F	KEYMGR sync all IPSec SA to Flow exit.	03/24	set	deviceconfig system	admin	03/24
UUID	564D0A8E-7D8A-4A3C-	Coopie installed	17:28:29		type		17:07:02
VMライセンス	04b3-1EFF2C88b63D	Coning installed	17:28:29	set	deviceconfig system	admin	03/24
VM モード	VMWare ESVi	KEYMGR sync all IPSec SA to Flow started.	03/24				17.00.57
ソフトウェア パージョン	810 b)		17:28:29		_	_	
	0.0.0	User admin logged in via Web from 192.168.55.1 using https	03/24	<u>цуу</u>			3 X
GiobalProtect エージェント	0.0.0		17120123	ロック未検出			

4. ネットワーク設定

ゾーンやインターフェイス及びルーティングなどのネットワーク設定を行います。

4.1. Virtual Wire 設定の削除

デフォルト状態で Virtual Wire の設定が存在しているかもしれません。

本ガイドでは Virtual Wire 設定は利用しませんので、もし存在していたら、設定を削除します。

(1) a)「Network」 \rightarrow b)「バーチャルワイヤー」 \rightarrow c)「default」を選択して、d)「削除」をクリックします。

paloalto	Dashboard ACC	Monitor Policies	Objects Network	Device	舎 コミッ	ト 💣 🖓 Config 🗝 🔍 検索
						ら ⑦ヘルプ
インターフェイス	٩					1個の項目 ラ 🗙
アイソーン NAN 空バーチャルワイヤー b)	🔲 名前	インターフェイス 1	インターフェイス 2	タグを許可	マルチキャスト ファイアウォ ール設定	リンク状態パス スルー
1000000000000000000000000000000000000	✓ default C)	ethernet1/1	ethernet1/2	default		

(2) 「はい」をクリックします。



4.2. ゾーンの設定

ゾーンは、物理または仮想インターフェイスをグループとして扱うための設定です。

ゾーンによって、異なるゾーン間の通信制御や同一ゾーン内の通信制御を、個別に行うことができるようになります。

以降、ネットワーク構成通りに、TrustとUntrust ゾーンを設定します。

(1) a)「Network」 \rightarrow b)「ゾーン」 \rightarrow c)「追加」をクリックします。

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Devic	е		🍐コミット 💣 🌡	🖗 Config 👻 🔍 検索
												🖸 🕢 ヘルプ
エインターフェイス	٩											0個の項目s → 🗙
Per Vーン b)												
 パーチャル ワイヤー 仮想ルーター 		名前	タイプ	イン 仮想	ターフェイス/ ミシステム	ゾーン プロテクジョン プロファイ	シ パケット レ 保護	バッファ	ログ設定	有効	含まれるネットワ ーク	除外されるネット ワーク
● IPSec トンネル デ DHCP デ DNS プロキシ ● C GlobalProtect ▲ QoS ● LLDP ▶ (日本)・ワーク プロファイル		c)										
	÷	追加 3 削除										

(2) 表示された画面で、a)名前に「Trust」、b)タイプで「レイヤー3」を選択して、b)「OK」をクリックします。



- (3) 同様の方法で、「Untrust」ゾーンも設定します。
- (4) 以下は、TrustとUntrustの2つのゾーンが生成された状態です。

paloalto	Dashbo	oard	ACC	Monitor	P	olicies	Objects	Network	Device				📥 コミット	💣 🛯 🥦 Config 👻 🔍 i	検索
														S 0)ヘルプ
■ インターフェイス														2 個の項目s	→ ×
(単 ゾーン 素 VI AN													ユーザ	- ID	
P科 ゾーン 勢 VLAN 全 バーチャル ワイヤー	名前	タイプ	インターフ	ェイス/仮想シス	ステム	ゾーン ブ	ロテクション プ	コファイル	パケット バッファ	呆護 ログ	設定	有効	ユーザ 含まれるネットワーク	- ID 除外されるネットワ	-2
 (単 ゾーン VLAN ① パーチャル ワイヤー ④ 仮想ルーター 	名前 Trust	タイプ layer3	インターフ	ェイス/仮想シス	ステム	ゾーン ブ	ロテクション プ	コファイル	パケット バッファ	呆護 ログ	設定	有効	ユーザ 含まれるネットワーク 任意	- ID 除外されるネットワ なし	-2
(単 ゾーン	名前 Trust	タイプ layer3	インターフ	ェイス/仮想シス	ステム	ゾーン ブ	ロテクション プ	コファイル	パケット バッファ	呆護 ログ	設定	有効	ユーザ 含まれるネットワーク 任意	- ID 除外されるネットワ なし	-2

4.3. インターフェイスの設定

インターフェイスにゾーン及び IP アドレスを割り当てます。

また、そのインターフェイスへの Ping の応答を許可する設定も行います。

paloalto	Dashboard	ACC Monitor	Policies	Objects	Network	Device			ミット 省 闷 Config -	♀検索
				L	a)				5	・ ③ヘルプ
	Ethernet VLAN	ループバックト	ンネル							
S VLAN	٩								9 個の項目	🗈 🔿 🗙
 	インターフェイス	インターフェイス タイプ	管理プロファイル	リンク状態	IP アドレス	仮想ルーター	タグ	VLAN / バーチャル ワイヤー	セキュリティ ゾーン	機能コ
IPSec トンネル	ethernet1/1	C)		Ē	none	none	Untagged	none	none	
T DHCP DNS プロキシ	ethernet1/2			Ē	none	none	Untagged	none	none	
▷ SolobalProtect	ethernet1/3			i	none	none	Untagged	none	none	
💑 QoS	ethernet1/4			m	none	none	Untagged	none	none	
	ethernet1/5			i	none	none	Untagged	none	none	
	ethernet1/6			m	none	none	Untagged	none	none	
	ethernet1/7			i	none	none	Untagged	none	none	
	ethernet1/8			i	none	none	Untagged	none	none	
	ethernet1/9			i	none	none	Untagged	none	none	
	🖶 サブインターフ:	ェイスの追加 😑 削除								

(2) a)インターフェイスタイプで「レイヤー3」を選択します。

まず、b)「設定」タブ内の設定を行います。

c)仮想ルーターで「default」を選択します。(※「default」仮想ルーターは後ほど設定します。)

d)セキュリティゾーンは「Untrust」を選択します。

Ethernet インターフェイス	0
インターフェイス ethernet1/1	
ね コメント	
インターフェイス レイヤー3 a)	~
タイプ Netflow プロファ None	~
b) イル 設定 IPv4 IPv6	
- インターフェイスの割り当て先	
仮想ルーター default C)	
セキュリティゾー Untrust d) ン	
	_
・	L

(3) a)「IPv4」タブをクリックします。
 b)「追加」をクリックします。

ネットワーク構成に従って、ethernet1/1 に設定する IP アドレス:c)192.168.55.20/24 を入力します。

Ethernet インター	-フェイス	0
インターフェイス名	ethemet1/1	
コメント		
インターフェイス タイプ	レイヤー 3	-
Netflow プロファイ	None	-
設定 IPv4	IPv6 詳細	
91:	プ 💿 スタティック 🔿 PPPoE 🔿 DHCP クライアント	
IP √ 192.168.55.2	_{0/24} C)	
b) ● 追加 ● 削隊	★ O FA	
IP アドレス/ネットマス	ク(例: 192.168.2.254/24)	_
		セル

(4) a)「詳細」タブをクリックします。

管理プロファイルの b)プルダウンをクリックして表示された c)「管理プロファイル」をクリックします。

Ethernet インターフェイス	0
インターフェイス ethernet1/1	
コメント	
インターフェイス レイヤー3	-
タイフ Netflow プロファ None	~
設定 IPv4 IPv6 詳細	
リンク設定	
リンク速度 auto リンクデュ auto ■ プレックス マレックス マリンク状態 ■ ■ ■	r
その他の情報 ARP エントリ ND エントリ NDP プロキシ LLDP	
管理プロファイル None b) ・	~
TPv4 MSS 調整 40	
IPv6 MSS 調整 60	
□ タグのないサブインターフェイス	
OK ++*>	セル

(5) 「このインターフェイスに対して、Ping は許可したい」という要件を想定して、その設定を行います。 a)名前に「Ping」、Permit Services 内の b)Ping にチェックを入れて、c)「OK」をクリックします。

インターフェイス管理プロファイル	0
名前 Ping a) Administrative Management services HTTP HTTPS Temperature SSH	アクセス許可 IP アドレス
ネットワークサービス Ping b) HTTP OCSP SNMP 広答ページ ユーザー ID ユーザー ID Syslog リスナー SSL ユーザー ID Syslog リスナー UDP	 送加 ・ にに Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::64
	C) OK キャンセル

(6) 「OK」をクリックします。 Ethernet インターフェイス 0 インターフェイス名 ethernet1/1 コメント -インターフェイス レイヤー3 タイプ Netflow プロファイ None ル 設定 IPv4 IPv6 詳細 リンク設定 リンク速度 auto リンク デュ auto プレックス リンク状態 auto \mathbf{w} その他の情報 ARP エントリ ND エントリ NDP プロキシ LLDP 管理プロファイル Ping MTU [576 - 1500] ¥ TCP MSS の題務 IPv4 MSS 調整 40 IPv6 MSS 調整 60 🦳 タグのないサプインターフェイス キャンセル OK

(7) ethernet1/2 に対しても、ネットワーク構成に従って、同様の設定を行います。

(ethernet1/2 のゾーンは Trust、IP アドレスは 192.168.45.20/24 です。)

4.4. ルーティング

「default」という名前の仮想ルーターが、PA Firewall 内部に元々存在しています。

仮想ルーターは、PA Firewall 内部でルーティングを行うための機能です。

「インターフェイスの設定」のセクションで、ethernet1/1 と 1/2 を仮想ルーターに割り当てたので、その 2 つのインターフェイス間のルーティングはできる状態になっています。

しかし、デフォルトルートは設定していないため、インターネットへのアクセスができる状態にはなっていないので、その設定を行います。

(1) a)「Network」 \rightarrow b)「仮想ルーター」 \rightarrow c)「default」をクリックします。

paloalto		Dashboard		ACC	Monit	or Policies	Objects	Ne	etwork	Device	•		🍐 コミット 💣 🌡	🎙 Config 🗸 🔍 検索
														ら のヘルプ
エ インターフェイス	٩													1 個の項目 🔿 🗙
IPM ゾーン 桑 VIAN		名前		インターフェ	イス	設定	RIP		OSPF		OSPFv3	BGP	マルチキャスト	ランタイム状態
●		default	c)	ethernet1/1 ethernet1/2		ECMP の状態: 無効								詳細ランライム状態
IPSec トンネル ア DHCP														
DNS プロキシ	4													
Concept														
▶ 📴 ネットワーク プロファイル														
	÷	追加 😑 削除												

(2) a)「スタティックルート」→ b)「追加」をクリックします。

仮想ルーター - default		0 🗆
Router Settings	-D.4 ID.4	
スタティック ルート	a)	
再配信プロファイル	ネクスト ホップ ホップ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	0個の項目s → ×
RIP	■ 名前 宛先 インター タイプ 値 管理距離 メト	リッ BFD ルートテ
OSPF	<u>-</u>	
0SPFv3		
BGP		
マルチキャスト		
	b)	
		OK キャンセル

 (3) a)名前に「default_route(任意)」、b)宛先に「0.0.0.0/0」、c)インターフェイスは「ethernet1/1」を選択、 d)ネクストホップへは、デフォルトゲートウェイの IP アドレス: 192.168.55.2 を入力します。
 e)「OK」をクリックします。

仮想ルーター-フ	、タティックルート - IPv4 ⑦	
名前	default_route	a)
宛先	0.0.0/0	b)
インターフェイス	ethernet1/1	c)
ネクスト ホップ	IP アドレス	d)
	192.168.55.2	
管理距離	10 - 240	
メトリック	10	
ルート テーブル	++7∠P	
BFD プロファイル	Disable BFD	
🗧 🗆 パス モニタリ	ング	
	失敗条件 • いず · すべ プリエンプティブ ホールド 2 れか て タイム (分)	
🔲 名前	有効化 送信元 IP 宛先 IP Ping 間隔 (秒) Ping 数	
●追加●問題		
	е) ок + +>t	

(4) 「OK」をクリックします。

仮想ルーター - default									0 🗖
Router Settings									
スタティック ルート	1 1 1 1 1 1								
再配信プロファイル	.				1. + - ?		1		1個の項目 → 🗙
RIP	■ 夕始	穷生	110-7-17	497			V L II w A	RED	∥_⊾=_ / ∥
OSPF	default_route	0.0.0.0/0	ethernet1/1	ip-address	192.168.55.2	default	10	None	unicast
OSPFv3									
BGP									
マルチキャスト									
	●追加 ■削除	8 = Ľ–							
									OK キャンセル

- (5) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (6) Commit 後、a)「Network」 → b)「インターフェイス」を確認すると、リンク状態が変化します。 以下は、インターフェイスが Link Up している状態です。

paloalto	Dashboard	ACC Monitor	Policies	Objects	Network [Device		≧ コミッ	· ト 💣 🖓 Config 🕶 C	~ 検索
									ର (シ ヘルプ
■インターフェイス b)	Ethernet VLAN	ループバックトン	ノネル							
レーン S VLAN		1	_						9 個の項目s	→ 🗙
€a バーチャル ワイヤー ④ 仮想ルーター	インターフェイス	インターフェイス タイプ	管理プロファイル	リンク状態	IP アドレス	仮想ルーター	タヴ	VLAN / バーチャル ワイヤー	セキュリティ ゾーン	機能
(値 IPSec トンネル	ethernet1/1	Layer3	Ping		192.168.55.20/24	default	Untagged	none	Untrust	
更 DHCP 型 DNS プロキシ	ethernet1/2	Layer3	Ping	Ē	192.168.45.20/24	default	Untagged	none	Trust	

5. NAT

本ガイドでは、Trust ゾーンのサブネット: 192.168.45.0/24 の端末から Untrust 方向(インターネット方向)へは、送信元ア ドレスを、ethernet1/1 に設定された IP アドレス: 192.168.55.20 にアドレス変換して通信することにします。

その設定方法を以下に示します。

(1) a)「Policies」 \rightarrow b)「NAT」 \rightarrow c)「追加」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network Dev	ice	📥 コミット 🧉 阔	Config 🗸 🔍 検索
									ら のヘルプ
	٩								0個の項目s 🔁 🗙
Solution Solution								変換済みパケット	
ポリシー ベース フォワーディング の 第日	名前	タグ	送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレス	宛先アドレス ▽ サービス	送信元変換 宛先変換	
 25 26 27 26 27 <li< th=""><th>4</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></li<>	4								
アプリケーション オーバーライド の証									
使 DoS プロテクション	C)								
	🕂 追加 目 削除	0 i Ľ–	✔ 有効化 💿	無効化 移動 -	■ 使用されていた	ミいルールの強調表示			

(2) a)「全般」タブで、b)名前に「outbound NAT (任意)」と入力します。

NAT ポリシール・	- אר
全般元のパク	アット 変換済みパケット
名前	outbound NAT b)
内容	
タグ	
NAT タイプ	ipv4
	ОК + +>セル

(3) a)「元のパケット」タブをクリックします。
 送信元ゾーンを追加します。b)「追加」 → c)「Trust」を選択します。
 宛先ゾーンとして、d)「Untrust」を選択します。

NAT ポ!	リシールール			0
全般	元のパケット	変換済みパケット		
🔲 lug	ส) รึกภ	苑先ゾーン	🗹 いずれか	🗹 いずれか
3 送(信元ゾーン 🔺	Untrust C)	🔲 送信元アドレス 🔺	■ 宛先アドレス ▲
in the	Trust C)			
		死先インターフェイス anv		
		0.17		
		サービス		
b)	7	any		
🛨 追加	ロ = 削除		●追加	● 追加 ● 削除
	×			OK キャンセル

 (4) a)「変換済みパケット」タブをクリックします。
 b)変換タイプに「ダイナミック IP 及びポート」、c)アドレスタイプに「インターフェイスアドレス」、d)インターフェイスに 「ethernet1/1」、e)IP アドレスに「192.168.55.20/24」を選択します。
 f)「OK」をクリックします。

NAT ポリ	リシールール					0
全般送信元	元のパケット アドレスの変換	変換済みパケット a)		宛先アドレスの変換		
	変換タイプ ダイ:	ナミック IP およびポート	b) 🕶	変換タイプ	None	-
7	ドレスタイプ イン	ターフェイス アドレス	c) 🚽			
イン	ターフェイス ether	met1/1	d) 🗸			
	IP アドレス 192.	168.55.20/24	e) 🚽			
					f) ок	キャンセル

(5) 以下は、NAT 設定後の状態です。

paloalto	Dashboard	ACC	Monito	r Policie	s Objects I	Network De	vice			
■ セキュリティ 参 NAT ▲ QoS	۹.				元のパケ	۲. ۲			変換済みバウ	ry þ
😽 ポリシー ペース フォワーディング	名前	タグ	送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換	宛先変換
 	1 outbound NAT	none	pag Trust	pa) Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 192.168.55.20/24	none

6. 全許可ポリシーの設定

デフォルトのポリシーのままでは、ゾーン間通信は許可されていないので、Trust ゾーンの端末から Untrust ゾーン方向(インターネット方向)への通信はできません。

よって、全てを許可するポリシーを一時的に設定し、インターネットへの通信ができるようにして、通信確認を行います。

6.1. [参考] 「ルールの使用状況」カウンター

PAN-OS8.1 から、ポリシー画面に「ルールの使用状況」のカウンター値が追加されました。

a) 「Policies」 \rightarrow b) 「セキュリティ」で表示された画面の c)の部分です。

paloalto		Dashboard	AC	С	Monitor	Pol	icies	Objects	Network D	evice			\$	コミット 💰 🍞	Config - 9. 検索
															5 ③ヘルプ
■ セキュリティ b)	٩					_									2 佃の項目5 📑 🗶
SP NAT					1			送信元		,	16 9.		ルールの使	用状況	c)
ネリシー ベース フォワーディン		名前		97	タイプ	ソーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	ヒット数	最後のヒット	最初のヒット	アプリケーショ
◎ 復号	1	intrazone-default	•	none	intrazone	any	any	any	any	(intrazone)	any	0			any
 ・シネル検査 ・・ションオーバーライ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	2	interzone-default	9	none	interzone	any	any	eny	any	any	any	0	1.		any

この「ルールの使用状況」には、このルールがいつ使われて、何回ヒットしたのか、という数が記録されます。

PA Firewall の運用を開始してしばらくすると、ポリシーの追加作業でいつのまにかポリシー数が大量に増えてしまい、使われていないポリシーを消したいが、どれが使われていないのかの判断が難しい、という場合があります。

そのような場合に、このカウンターを見ることで、不要なポリシーかどうかの判断がつきやすくなります。

運用面ではとても便利な機能ですが、本ガイドでは、紙面の物理的な横幅の都合上、スクリーンショットでポリシーをすべて表示すると文字が小さくなりすぎるため、一時的に非表示にすることにします。

[参考]非表示にする方法(必ずしも実施する必要はありません):

いずれかの列の、例えば「アドレス」列の a)「▽」 → b)「カラム」で表示された中から「ルールの使用状況~」の 3 つのチェックを外します。

							送信元			18先	a)				
	名前		タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	▽ アプリケーショ	2	サービス	アクション	プロフ
1	intrazone-default	•	none	intrazone	any	any	any	any	(intrazone)	any	🗰 лэд b)		名前		
2	interzone-default		none	interzone	any	any	any	any	any	any	別の課務		タグ		
											1.0 ×2 100 20E		タイプ		
													送信元 ゾーン		
													送信元 アドレ	z	
													送信元 ユーサ	-	
													送信元 HIP フ	ロファイル	
													宛先 ゾーン		
													宛先 アドレス	6	
													ルールの使用	状況 ヒット数	C)
													ルールの使用	状況 最後のヒッ	4
													ルールの使用	状況 最初のヒッ	1
												V	アプリケーシ	ョン	

6.2. 設定

すべてを許可するポリシーを設定します。

(1) a)「Policies」 \rightarrow b)「セキュリティ」 \rightarrow c)「追加」をクリックします。

paloalto	٦	Dashboard ACC	Ν	Ionitor	Policies	Obje	cts N	etwork Devic	е				📥 コミッ	ト 🔓 😡 Confi	g ▼ Q.検 索
															ら ③ヘルプ
📾 セキュリティ b)	٩													2個	の項目s 🔿 🗙
🗊 NAT							送信元			昆先					
👺 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	intrazone-default 🔮	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可	none	none
 ドンネル検査 アプリケーション オーバーライド 	< 2	interzone-default 🧇	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none
🈓 RII															
€DoS プロテクション	6	c)													
	•	追加 🖃 削除 💿 コピー	- 🌤 オ	ーバーライト	* ※ 戻す	🕑 有効化	💽 無効化	移動 - 📔 使用さ	れていないル	ールの強調者	表示				

(2) a)「全般」タブで、b)名前に「allow outbound (任意)」と入力します。

セキュ	リティポ	リシールール	r				0
全般 a)	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	
	名前	allow outbound		b)			
л	ール タイプ	universal (defau	lt)				-
	内容						
	タグ						-
						OK キャン	セル

(3) a)「送信元」タブで、b)「追加」をクリックし、c)「Trust」を選択します。



(4)「ユーザー」タブは、デフォルトのまま「any」とします。
 (※User-ID 連携を行った場合に、ユーザ名でポリシー制御を行う場合は、このタブで設定します。)

セキュ	セキュリティ ポリシー ルール で										
全般	送信元	ユーザー	宛先	アプリケーシ	コン	サービス/URL カテゴリ	アクション				
any III 送	信元ユーザー	▼			any	▼ P プロファイル▲					
争 追加	a 🖨 Kiak				+ 追						
- Communities							OKキャン	セル			

(5) a)「宛先」タブで、b)「追加」をクリックし、c)「Untrust」を選択します。

セキュ	リティポリ	リシールーノ	r					0
全般	送信元	ユーザー	宛先 a)	アプリケーショ	ョン	サービス/URL カテゴリ	アクション	
選択		-		1	V IN	『れか		
二 宛:	先ゾーン ▲				■ 宛	先アドレス ▲		
	Untrust	C)						
b)								
🖶 追加	□ ■ 削除				🕂 追加	🛛 🖃 削除		
					Neg	ate		
							DK ++721	セル

(6) 「アプリケーション」タブは、デフォルトのまま「いずれか」とします。

セキュ	セキュリティ ポリシー ルール の											
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション						
🗹 U1	ずれか											
7	プリケーショ	ン 🔺					٩,					
🕂 追加	加 🖃 削除											
						OK キャンセ	N					

(7) a)「サービス/URL カテゴリ」タブで、サービスは b)「any」を選択します。

セキュ	リティポリ	リシールーノ	r					0
全般	送信元	ユーザー	宛先	アプリケーシ	/ヨン	サービス/URL カテゴリ	アクション	
any	t) - ((🗹 113	。 パカか		
サ・	-ピス ▲				UR	∟ カテゴリ 🔺		
● 追加	0 🗖 削除			_	月 油力	□ ■ 削除		-1
							OK キャンセ	:16

(8) a)「アクション」タブはデフォルト設定のままとします。

(デフォルト状態で、アクションは「Allow」、ログ設定は「セッション終了時にログ」となっています。) b)「OK」をクリックします。

セキュ	リティポリ	シールーノ	L						0
全般	送信元	ユーザー	宛先	アプリケー	ション	サービス	/URL カテゴリ	アクション	<u> </u>
アクシ	ヨン設定				ログ目	设定		aj	
	アクシ	ヨン Allow	送信到達	不能		ログ転送	 セッション開始 ✓ セッション終う None 	台時にログ 了時にログ	-
プロフ	ファイル設定				その	も の設定 スケジュール	None		-
	7ロファイル タ・	17 None			Q	oS マーキング	None	ポンス検査の無効化	•
2							b)	ОК + +>	セル

(9) Trust から Untrust への通信を全許可するポリシー設定が完了した状態です。

	名前	タヴ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
1	allow outbound	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	any	🕑 許可	none	
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
3	interzone-default	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none

(10)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

6.3. 通信確認

- (1) Trust ゾーン: 192.168.45.0/24 上のクライアント PC から、Google や YouTube などのインターネット上の Web サイトヘアクセスできることを確認します。
- (2) a)「Monitor」→ b)「トラフィック」で表示される、c)のログを確認します。
 (1)で実施した、クライアント PC からインターネットサイトへアクセスしたログが出力されます。

paloalto	Da	shboard	ACC	Monitor	Policies	Objects	Network	Device				â コミッ	ト 💣 🖓 Config 🗸	Q 検索
				a)								4		
viady iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由	
QURL フィルタリング	₽ <u>c</u>)	02/07 22:54:41	end	Trust	Untrust	192.168.45.32		172.217.31.132	443	google-base	allow	allow outbound	tcp-fin	7.9k
NildFireへの送信	Þ	02/07 22:54:41	end	Trust	Untrust	192.168.45.32		172.217.31.131	443	google-base	allow	allow outbound	tcp-fin	77.6k
III データ フィルタリング	Þ	02/07 22:54:41	end	Trust	Untrust	192.168.45.32		172.217.31.162	443	google-base	allow	allow outbound	tcp-fin	7.0k
III ユーザー ID	Þ	02/07 22:54:41	end	Trust	Untrust	192.168.45.32		172.217.31.141	443	google-base	allow	allow outbound	tcp-fin	11.8k

7. SSL/TLS 復号化の設定

現在のインターネット通信の半数またはそれ以上が SSL/TLS となり、今後もこの流れは加速することが予想されます。

SSL/TLS によって暗号化された通信は、Firewall で脅威を検知することが困難なため、脅威検知すべきトラフィックは復号化が必要です。

以下は、PA Firewall による SSL/TLS 復号化の動作概要です。



SSL 復号化は、「Web サイト~PA Firewall 間」の SSL セッション (SSL セッション-A) と、「PA-Firewall~クライアント間」の SSL セッション (SSL セッション-B) はそれぞれ別々に確立されます。

中間に入る PA Firewall は、受け取ったデータを復号化し、再び暗号化して送り出す、という処理を行います。

以下は、その処理フローの概要です。

- (SSL セッション確立前の) SSL ハンドシェークの段階で、PA Firewall が Web サイト(www.acme.com)からの証明 書を受け取る。
- ② PA Firewall がその証明書の内容を一部書き換え、PA Firewall 内の秘密鍵で署名を行う。
- ③ PA Firewall は、クライアント PC との SSL ハンドシェークで、PA Firewall が署名した証明書をクライアントに送り出す。
- ④ クライアント PC は、PA Firewall で生成したルート証明書を持っているので、③で受け取った証明書を信頼する。
- ⑤ 「Web サイト~PA Firewall 間」と「PA-Firewall~クライアント間」で、それぞれ異なる SSL ハンドシェークが行われる。
- ⑥ SSL ハンドシェークが完了すると、「Web サイト~PA Firewall 間」と「PA-Firewall~クライアント間」で、それぞれ 異なる SSL セッションが確立される。
- ⑦ その結果、PA Firewall 内では、通信データは復号化されるので、脅威の有無をチェックすることができる。

以降、PA Firewall の SSL/TLS 復号化の設定を行います。

7.1. ルート証明書の生成

PA Firewall がインターネットに存在する Web サイトのサーバー証明書を受け取り、それを書き換えてクライアントに送り 出すためには、PA Firewall 内に認証局の秘密鍵が必要です。

本ガイドでは、PA Firewall が認証局となり、PA Firewall 自身でルート証明書及び秘密鍵を生成することにします。 (自社内に認証局がある場合、そのルート証明書及び秘密鍵を PA Firewall にインポートして利用することもできます。)

(1) a)「Device」 \rightarrow 「証明書の管理」の下の b)「証明書」 \rightarrow c)「生成」をクリックします。

paloalto	Dashboard	ACC Monit	or Policies	Objects	Network Device			参コミット d	🔋 👰 Config 🗸 🔍 検索
					<u>a)</u>	J			😋 💿 ヘルプ
↓ セットアップ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	デバイス証明書	デフォルトの信頼	頂された証明機関						
									0 個の項目s 🔿 🗶
く パスリート フロファイル 各 管理者	□ 名前	サブジェクト	発行者	CA	+-	有効期限	状態	アルゴリズム	用途
20 管理者ロール 20 管理者ロール 20 営理者ロール									
器 認証シーケンス ユーザー ID									
Q VM 情報ソース ▼ ○ 500 500 500 500 500 500 500 500 500 5	4								
 証明書 b) 									
OCSP レスポンダ									
👸 SSL/TLS サービス プロフォ 🌆 SCEP		_							
			c)						
	■ 削除 無効化 5	恵新 📥 インポート 🥫	生成 📩 エクスポー	—ト 📥 HA キー0	Dインポート 🔚 HA キーの:	エクスポート			

(2) a)証明書名に「SSL-Forward-Proxy-Trust-CA (任意)」、b)共通名に「SSL-Forward-Proxy-Trust-CA (任意)」、
 c)「認証局」にチェックを入れます。

d)「OK」をクリ	ックします。		
証明書の生成		0	
証明書タイプ(・ ローカル O SCEP		
証明書名	SSL-Forward-Proxy-Trust-CA		a)
共通名	SSL-Forward-Proxy-Trust-CA		b)
署名者	明響に表記される IP または FQDN	~	
	🛛 認証局		C)
OCSP レスポンダ		~	
▲ 暗号設定			
アルゴリズム	RSA	~	
ビット数	2048	~	
ダイジェスト	sha256	~	
有効期限(日)	365	- 11	
証明書の属性			
🔲 タイプ	値		
● 追加 ■ 削除		- 11	
	d) _{生成}	キャンセル	

(3) 証明書の生成が成功したことを示すメッセージが出ます。「OK」をクリックします。



7.2. ルート証明書の用途設定

インターネット上の Web サイトが持つ SSL 証明書が、「信頼された証明書」、「信頼されない証明書」のどちらでも、PA Firewall で生成したルート証明書:「SSL-Forward-Proxy-Trust-CA」と秘密鍵を使って、「PA Firewall~クライアント PC 間」の SSL ハンドシェークを行う、という設定を行います。

(1) 生成した「SSL-Forward-Proxy-Trust-CA」をクリックします。

	Dashboard ACC	Monitor Policies	Objects Network	Device			📥 コミッ	ト 💣 阔 Config •	● Q 検索
⊡⊠ ユーザー ID	デバイス証明書 デフ	オルトの信頼された証明相	機関					c	:
● VM 済戦リース ▼ ■ 証明書の管理 ■ 証明書								1 個の項	E → X
■ 証明書プロファイル ■ 証明書プロファイル ■ OSSP レスポンダ	□ 名前 □ 同 SSL-Forward-Proxy-1	サブジェクト irust-CA CN = SSL-Forward	·Proxy-Trust-CA CN = SSL-F	orward-Proxy-Trust-CA	*-	有効期限 Feb 28 09:43:01 2019 GMT	<u>状態</u> 有効	アルゴリズム RSA	用途
 SSL/TLS サービス フロファイル 「国 SCEP ・ ・	4				1		I	1	
	🖃 削除 無効化 更新 📥	インポート 👼 生成 🚢 エク	'スポート 📥 HA キーのインポ	ニート 🔮 HA キーのエクスポート					

(2) a)「フォワードプロキシ用の信頼された証明書」および「フォワードプロキシ用の信頼された証明書」にチェックを入れ、
 b)「OK」をクリックします。

名前	SSL-Forward-Proxy-Trust-CA
サブジェクト	/CN=SSL-Forward-Proxy-Trust-CA
発行者	/CN=SSL-Forward-Proxy-Trust-CA
発効日時	Feb 28 09:43:01 2018 GMT
有効期限	Feb 28 09:43:01 2019 GMT
アルゴリズム	RSA
	☑ 認証局
	✓ フォワードプロキシ用の信頼された証明書
	☑ フォワード プロキシ用の信頼されない証明書
	信頼されたルート CA
7.3. 証明書のエクスポートとインポート

PA Firewall からルート証明書をエクスポートして、それをクライアント PC ヘインポートします。

7.3.1. 証明書のエクスポート

「信頼された証明書」用のルート証明書をエクスポートします。 (次のセクションで、このルート証明書をクライアント PC ヘインポートします。)

(1) a)「SSL-Forward-Proxy-Trust-CA」が選択された状態で、b)「エクスポート」をクリックします。

paloalto	Dashboard	ACC M	onitor Policies	Objects	Network Device						🏝 コミット 🧉 🖓 Config 🗸 🔍 検索
											😋 🔞 ヘルプ
III ユーザー ID Ø VM 情報 V ース	デバイス	証明書 デフォル	トの信頼された証明機	関							
▽ 😭 証明書の管理											1 個の項目 🔿 🗶
6回 証明書 同 証明書プロファイル 同 OCSP レスポンダ	🗌 名前		サプジェクト	5	発行者	СА	*-	有効期限	状態	アルゴリ ズム	用途
🔒 SSL/TLS サービス プロファイノ), 🗹 🛛 🕫 SS	SL-Forward-Proxy-Trust-	CA CN = SSL-Forward-Prox	y-Trust-CA C	CN = SSL-Forward-Proxy-Trust-CA	☑		Feb 28 09:43:01 2019 GMT	有効	RSA	フォワード プロキシ用の信頼された証明書
SCEP	'										フォワード プロキシ用の信頼されない証明書
■ SSL 後方し例か ■ 広告ページ ■ ログ設定 ■ サーバー ブロファイル			b)							
	● 削除無	効化 🏾 更新 📥 イン	ポート 🛛 🥦 生成 📥 エクス	スポート 📥 🛚	HA キーのインポート 🔚 HA キー	- の エ:	クスポー	<u>۲</u>			

(2) a)ファイルフォーマットで「Base64 エンコード済み証明書(PEM)」を選択して、b)「OK」をクリックします。



(3) エクスポートされたルート証明書を、一時的にコンソール PC へ保存しておきます。

7.3.2. クライアント PC ヘルート証明書をインポート

PA Firewall からエクスポートしたルート証明書を、Trust ゾーンのクライアント PC ヘインポートします。

このことで、PA Firewall が再生成したサーバー証明書を、クライアント PC が信頼できるようになります。

- (1) PA Firewall からエクスポートしたルート証明書を、クライアント PC(例: Windows7) ヘコピーします。
- (2) そのファイルをダブルクリックして表示された画面で、「Install Certificate / 証明書のインストール」をクリックします。

Certificate						
General Details Certification Path						
Certificate Information						
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.						
Issued to: SSI-Forward-Proxy-Trust-CA						
Issued by: SSL-Forward-Proxy-Trust-CA						
Valid from 2018/02/04 to 2019/02/04						
Install Certificate						
ОК						

(3) 「Next / 次へ」をクリックします。



(4) 「Place all certificate in the following store / 証明書を全て次のストアに配置する」を選択して、「Browse…/参照」を クリックします。



(5) 「Trusted Root Certification Authorities / 信頼されたルート証明機関」を選択して、「OK」をクリックします。

Select Certificate Store					
Select the certificate store you want to use.					
Personal					
Enterprise Trust					
Active Directory User Object					
Show physical stores					
OK Cancel					

(6) 「Next / 次へ」をクリックします。

Certificate Import Wizard	×				
Certificate Store					
Certificate stores are system areas where certificates are kept.	_				
Windows can automatically select a certificate store, or you can specify a location for the certificate.					
O Automatically select the certificate store based on the type of certificate					
Place all certificates in the following store					
Certificate store:					
Trusted Root Certification Authorities Browse					
Learn more about certificate stores					
<back next=""> Cance</back>	2				

(7) Finish をクリックします。



(8) 警告が出ますが、「Yes / はい」をクリックします。



(9) ルート証明書のインポートが完了しました。「OK」をクリックします。



7.4. SSL/TLS 復号ポリシーの設定

SSL 復号化を行うには、どのような条件(例:送信元や宛先)の場合に復号するのか、という復号ポリシーの設定も必要です。

まずは、全ての宛先に対して復号化するポリシーを設定します。

(1) a)「Policies」 \rightarrow b)「復号」 \rightarrow c)「追加」をクリックします。

paloalto	Das	shboard	ACC	Monitor	Policies	Objects	Network D	evice	솔 그 목	ット 省 阔 Con	fig ▼
											😋 🕢 ヘルプ
📾 セキュリティ	۹									0 復	圆の項目s ラ 🗙
₩ NAT a QoS						送信元			宛先		
一 ポリシー ベース フォワーディング		名前		タグ	ゾーン	アドレス	ユーザー	ゾーン	アドレス	URL カテゴリ	サービス
 · · · · · · · · · · · · · · ·											
III アプリケーション オーバーライド 分 認証	4										
(€DoS プロテクション											
	, , , , , , , , , , , , , , , , , , ,	-									
	_C)	_									
	🕂 追	加 😑 削除	<u>ତ</u> ସଥ-	- 📝 有効化 💿	無効化 移動 -	📕 使用されて	いないルールの強調者	示			

(2) a)「全般」タブで、b)名前に「Dec_Rule1 (任意)」と入力します。

復号ポ	リシール	ール				0
全般	送信元	宛先	サービス/URL カテゴリ	オプション		
<u> </u>	名前	Dec_Rule1	b)		
	内容					
	タグ					•
					ОК	キャンセル

(3) a)「送信元」タブで、b)「追加」をクリックし、c)「Trust」を選択します。

復号ポリシー ル	- <i>ル</i>				C
全般 送信元	宛先 サービ	ス/URL カテゴリ	オプション		
□ いずれか		🗹 いずれか		any	-
■ 送信元ゾーン ▲		🔳 送信元アドレス		🔳 送信元ユーザー 🔺	
. (22) Trust	C)				
D)		➡追加 ■削除		+追加 日間幕	
		Negate			
т.				OK	キャンセル

(4) a)「宛先」タブで、b)「追加」をクリックし、c)「Untrust」を選択します。

復号ポ	リシール・	ール			Ø
全般	送信元	宛先	サービス/URL カテゴリ	オプション	<u>ii</u>
L 113	ずれか	u)		🗹 いずれか	
2 宛	先ゾーン ▲			🔳 宛先アドレ	ג ▲
⊻ [20	Untrust	C)			
	_				
b)				0.1040 001	1120
+ 15/		-	_	H 15/11	ling
-					
					OK キャンセル

(5) 「サービス/URL カテゴリ」は、デフォルトのまま「Any」とします。

復号ポリシ	ールール			0
全般送	信元 宛先	サービス/URL カテゴリ	オプション	
any	-		🗹 いずれか	
🔲 サービス	ζ		🔲 URL カテゴ	ע 🔺
				196
	HIN		+ 25// ■ 8	uax
				OK キャンセル

(6) a)「オプション」タブで、b)アクションで「復号」を選択し、c)タイプが「SSL フォワードプロキシ」であることを確認します。
 d)「OK」をクリックします。

復号ポ	リシール・	- <i>I</i> L				0	
全般	送信元	宛先	サービス/URL カテゴリ				
	アクション 〇 復号なし 💿 復号 b)						
	タイプ SSL フォワード プロキシ C)						
復号プ	復号プロファイル None 🔍						
					d) ок	キャンセル	

(7) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

7.5. 通信確認

7.5.1. 「信頼された証明書」を持つサイトへの通信確認

ー般的なインターネット上の HTTPS サイトヘアクセスできること及びそのサーバー証明書の状態を確認します。

Chrome ブラウザの場合: Google が提供するサイト"以外"の HTTPS サイトで確認してください。 Chrome が Google 提供サイトへアクセスする場合には、初動として QUIC(UDP/443)を利用する場合が多く、v8.1 におい ても PA Firewall は QUIC の復号化をサポートしていないため、QUIC が通過する現段階では、復号化が動作しません。 後に QUIC を拒否する設定に変更します。

- (1) Trust ゾーン: 192.168.45.0/24 のクライアント PC の Web ブラウザ(例: Chrome)で、インターネットの HTTPS サイト (例: <u>https://www.paloaltonetworks.com</u>) ヘアクセスします。
- (2) Chrome ブラウザの a)「保護された通信」 → b)証明書の下の「有効」をクリックします。

保護された接続 × お客様がこのサイトに送信した消報 (バスワード、クレシットカード番号など) が第三者に見られることは ありません。詳しく見る Log in » Get Support Q B) ・ Flash 確認 (デフォルト) ▼	MENU
★ Flash 確認 (デフオルト) ▼	
A ware exploits and	

 (3) a)「*.paloaltonetworks.com」証明書の b)「Issued by / 発行者」が、PA Firewall で生成した「SSL-Forward-Proxy-Trust-CA」になっています。

	<参考> SSL 復号なしの場合の、本来の証明書
Certificate	Certificate
General Details Certification Path	General Details Certification Path
Certificate Information	Certificate Information
This certificate is intended for the following purpose(s):	This certificate is intended for the following purpose(s):
Ensures the identity of a remote computer Proves your identity to a remote computer	Ensures the identity of a remote computer Proves your identity to a remote computer
Issued to: *.paloaltonetworks.com a) Issued by: SSL-Forward-Proxy-Trust-CA b) Valid from 2017/07/11 to 2018/10/11	* Refer to the certification authority's statement for details. Issued to: *,paloaltonetworks.com Issued by: Symantec Class 3 Secure Server CA - G4 Valid from 2017/ 07/ 11 to 2018/ 10/ 11
Issuer Statement	Issuer Statement
OK	OK

PA Firewall が「*.paloaltonetworks.com」の正式な証明書を受け取り、その証明書の一部の情報を書き換え & ルートの秘密鍵で署名し直して、クライアント PC に渡しているので、このような証明書になります。

クライアント PC には事前に PA Firewall のルート証明書(SSL-Forward-Proxy-Untrust-CA)をインポートしたので、セキュリティの警告がでることなく、Web サイトをみることができます。

43

7.5.2. ログの確認

復号化されているかどうかを、ログから確認することができます。

(1) a)「Monitor」→ b)「トラフィック」→ c)ログの先頭の ^{「●} アイコンをクリックします。

paloalto		Dashboard A	CC	Monitor F	Policies (bjects Net	work Device	•		å] :	ミット 省 😡	Config - Q 検索
											手動	🚽 😪 💿 ヘルフ
v ind	٩											🗙 🖶 🎼 🚰
戦トラフィック D)		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	アプリケーション	アクション	ルール
GURL フィルタリング	Þ	c) 03/25 11:20:52	end	Trust	Untrust	192.168.45.32		66.151.25.23	443	ssl	allow	allow outbound
NildFireへの送信	130	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		66.151.25.23	443	ssl	allow	allow outbound
ー テータ フィルタリング	P	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		54.186.44.170	443	ssl	allow	allow outbound
III ユーザー ID	P	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		54.186.44.170	443	ssl	allow	allow outbound
🏠 トンネル検査	Þ	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		104.237.191.1	443	web-browsing	allow	allow outbound
◎ 設定	Ð	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		13.33.9.100	443	ssl	allow	allow outbound
R PP-A	Þ	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		13.33.9.100	443	ssi	allow	allow outbound

(2) SSL/TLS 復号されたトラフィックには、「復号化」にチェックが入っています。

詳細ログビュー			0 🗆
全般	送信元		宛先
セッション ID 2402 アクション allow アクションの送信 from-policy アブリケーション ssl ルール allow outbound セッション終了理 tcp-fin カテゴリ computer-and-internet-info の何期システム	送信元ユーザー 送信元 ポート ゾーン インターフェイス NAT IP NAT ポート	192.168.45.32 192.168.0.0-192.168.255.255 50464 Trust ethernet1/2 192.168.55.20 23768	 宛先ユーザー 宛先 66.151.25.23 国 United States ポート 443 ゾーン Untrust インターフェイス ethernet1/1 NAT IP 66.151.25.23 NAT ポート 443
デバイスのシリア ル音号 IP プロトコル tcp ログアクション 生成日時 2018/03/25 11:20:52 開始時間 2018/03/25 11:20:52 経過時間 (秒) 3 トンネル タイプ N/A	詳細 タイプ バイト 受信済みバイト 送信済みバイト 繰り返し回数 パケット 受信したパケット 送信したパケット 送信したパケット 送信元 UUID	end 8521 7212 1309 1 22 14 8	フラグ キャプティブ ボー タル プロキシ トランザ クション 復号化 グリア キャファ ヤーバーからクラ イアントから サーバーからクラ イアシートから サーバーからクラ イアシートから サーバーからクラ イアシートから サーバーからクラ イアシートから サーバーからクラ イアシートから サーバーからクラ イアシートから サーバーからクラ イアシーシ ション ション ション ション ション ション ション ション 除小された偵察 転送内容の復号化
PCAP 受信日時 タイプ ア・ ン	^{プリケーショ} アクション	ルール パイト 重大度	カテゴリ 判定 URL ファイル名
2018/03/25 11:20:52 end ssl	allow	allow 8521 outbound	computer- and- internet- info
			閉じる

7.5.3. 「信頼されない証明書」を持つサイトへの通信確認

「信頼されない証明書」を持つサイトへアクセスできること及びそのときのサーバー証明書を確認します。

- Trust ゾーン: 192.168.45.0/24 のクライアント PC の Web ブラウザ(例: Chrome)で、PA Firewall のマネージメントインターフェイス (<u>https://192.168.55.11</u>) ヘアクセスします。
- (2) Chrome の a)「保護されていません」 → b)証明書の下の「無効」をクリックします。



(3) 「Issued by / 発行者」が、PA Firewall で生成した「SSL-Forward-Proxy-Trust-CA」になっています。

	<参考>本来の証明書
Certificate	Certificate
General Details Certification Path	General Details Certification Path
Certificate Information	Certificate Information
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer • Proves your identity to a remote computer	Windows does not have enough information to verify this certificate.
Issued to: 73240dc89bc6d19959834891cbb15e422f2d53dd9 4b5f1d58d449f1b371c38d5 Issued by: SSL-Forward-Proxy-Trust-CA	Issued to: 73240dc89bc6d19959834891cbb15e422f2d53dd9 4b5f1d58d449f1b371c38d5 Issued by: localhost
Learn more about certificates	Learn more about certificates
ОК	ОК

信頼されない認証局から発行された証明書を持つ Web サイトの場合も、PA Firewall ~ クライアント PC 間で SSH セッションが確立されている=SSL 復号化が行われていることがわかります。

7.6. [参考]「信頼されない証明書」の場合には必ずセキュリティ警告を出す設定

ここまでの設定では、「信頼された証明書」も「信頼されない証明書」も、PA Firewall で生成した一つのルート証明書で SSL 復号化/暗号化を行う設定にしました。(「ルート証明書の用途設定(既述)」参照)

実はこの設定では、「信頼されない証明書」を持つ Web サイトへアクセスした場合にも、クライアント PC の Web ブラウザ がセキュリティ警告を出さないで、あたかも信頼された Web サイトとして認識してしまう場合があります。

それは、サーバー証明書の Common Name や Subject Alternative Name (以降、SAN) と、Web ブラウザに入力した URL の FQDN (または IP アドレス) が一致する場合です。

ここでは簡易的なテストとして、PA Firewallのマネージメントインターフェイスを使って試してみましょう。

7.6.1. マネージメントインターフェイス用のサーバー証明書の作成

7.6.1.1. 仮の認証局の生成

(1) a)「Device」 \rightarrow b)「証明書」 \rightarrow c)「生成」をクリックします。

paloalto	Dashboard ACC Monito	or Policies Objects	Network Device	1			4	ちコミッ	ト 💣 陽 Config 🗝 🔍 検索		
			a)						😋 🔞 ヘルプ		
	デバイス証明書 デフォルトの	D信頼された証明機関									
		1 僮の項目 🕂 🗶									
● 証明者 D)	□ 名前	サブジェクト	発行者	CA	*-	有効期限	状態	アルゴ リズム	用途		
🔒 SSL/TLS サービス プロファイル 国家SCEP	SSL-Forward-Proxy-Trust-CA	CN = SSL-Forward-Proxy-Trust-CA	CN = SSL-Forward-Proxy-Trust- CA			Feb 28 09:43:01 2019 GMT	有効	RSA	フォワード プロキシ用の信頼 された証明書		
B SSL 復号化例外 応答ページ											
□ ログ設定 ▼ 1 サーバー プロファイル		_									
SNMP トラップ		c)									
- J Systog	副削除 無効化 更新 🛓 インポー	ト 👼 生成 🚢 エクスポート 📩	HA キーのインポート 🚢 HA キー	ーのエク	スポー						

(2) 以下の通り設定し、仮の認証局を生成します。

証明書の生成		0	
証明書タイプ(ローカル SCEP 		
証明書名	dummy-CA		dummy-CA(任意)
共通名	dummy-CA		dummy-CA(任意)
	u明書に表記される IP または FQDN		
有合也	☑ 認証局	~	認証局にチェック
OCSP レスポンダ		~	
▲ 暗号設定			
アルゴリズム	RSA	-	
ビット数	2048	-	
ダイジェスト	sha256	*	
有効期限(日)	365		
証明書の属性			
917	11		
+ 追加 ■ 削除			
	生成	キャンセル	

7.6.1.2. マネージメント用サーバー証明書の作成

- (1) もう一度、a)「Device」 \rightarrow b)「証明書」 \rightarrow c)「生成」をクリックします。
- (2) 以下の通り設定し、サーバー証明書を生成します。

証明書の生成		0	
証明書タイプ	● ローカル ○ SCEP		
証明書名	dummy-cert01		dummy-cert01(任意)
共通名	192.168.55.11		192.168.55.11
署名者	dummy-CA		dummy-CA を選択
Ī	認証局		
OCSP レスポンダ		-	
▲ 暗号設定			
アルゴリズム	RSA	-	
ビット数	2048	~	
ダイジェスト	sha256	~	
有効期限 (日)	365		
証明書の属性			
□ タイプ	值		
IP IP	192.168.55.11		タイプに「IP」を選択、値に 192.168.55.11
🕂 追加 🕒 削除			
	生成年十	·ンセル	

(※↑「証明書の属性」のタイプに、IP または Host Name を指定することで、SAN 値として扱われます。)

7.6.1.3. マネージメントインターフェイスのサーバー証明書の変更

(1) a)「Device」 → b)「セットアップ」 → c)「管理」 → 一般設定の d) $\stackrel{\circ}{\longrightarrow}$ アイコンをクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	1	
[™] セットアップ b)	C) 管理 操	作 サービ	ス「インタ	-7113	テレメトリー	- コンテン	a) איזע Wild	Fire セッション	HSM
← 高可用性 ■ 設定監査 ● パスワード プロファイル	一般設定						d) *	Panorama設定	
 8 管理者 9 管理者ロール 8 認証プロファイル 	ホスト名 PA-VM ドメイン							Pano	orama へのデー
※ 認証シーケンス 10 ユーザー ID 2 いい 情報ソース		ログ	Panoral	ma に送信され					
▼ (副 証明書の管理 ■ 証明書 ■ 証明書 ■ 証明書プロファイル			331/1123 1/ -	- C ス ソロクアイ タイム ゾー 表示言	ン Asia/Tokyo 語 en				μ.

(2) a)「SSL/TLS サービスプロファイル」のプルダウンで表示された b)「SSL/TLS サービスプロファイル」をクリックします。

一般設定	Ø
ホスト名	PA-VM
ドメイン	
	DHCP サーバー提供のホスト名を受け入れる
	DHCP サーバー提供のドメインを受け入れる
ログイン パナー	
	ログインパナーの確認を管理者に強制
ssi/Tis #_ビス プロファ	
33L/1L3 リーヒス ノロノノ イル	None
タイム ゾーン	
表示言語	en
日付	2018/03/10
時間	10:48:33
緯度	
経度	
	□ コミット ロックの自動実施
	証明書有効期限チェック
	✓ ハイパーバイザによって割り当てられた MAC アドレスの
	使用
	GTP Security
	OK キャンセル

(3) a)名前に「dummy-ssl-profile(任意)」、b)証明書で「dummy-cert01」を選択し、c)「OK」をクリックします。

SSL/TLS サービスプロファイル 💿							
名前	dummy-ssl-profile	a)					
証明書	dummy-cert01 🗸	b)					
プロトコル設定		1					
最小パージョン	TLSv1.0						
最大パージョン	Max 💌						
	C) OK キャンセル						

- (4) さらに「OK」を押して、一般設定を閉じます。
- (5) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

(WebUI のサーバー証明書を変更したので、WebUI へのアクセスには再接続が必要です。)

7.6.2. 通信確認

- (1) クライアント PC の Web ブラウザから PA Firewall のマネージメントインターフェイス (<u>https://192.168.55.11</u>) ヘア クセスします。
- (2) 「保護された通信」として扱われてしまいます。

先ほど生成した「dummy-CA」は、誰からも信頼されていない認証局であり、 その認証局が署名した「dummy-cert01」証明書も、「信頼されない証明書」であるにも関わらず、信頼されています。

a)「保護された通信」→ b)証明書の「有効」をクリックします。



(3) 以下が、Web ブラウザが受け取ったマネージメントインターフェイスのサーバー証明書の状態です。



発行者/Issued by は「SSL-Forward-Proxy-Trust-CA」であるため、Web ブラウザにインポート済みなので、署名検証は OK と判断されます。

更に、Subject の Common Name は、192.168.55.11、SAN も IP Address=192.168.55.11 となっていて、Web ブラウ ザに入力した URL の IP アドレスと一致するので、Web ブラウザは、この証明書を「信頼できるサーバー証明書」として認 識してしまいます。

7.6.3. Web ブラウザがサーバー証明書を信頼する条件

Web ブラウザが SSL 通信を行う際、以下の条件のうち①は必須として、②か③が Web ブラウザに入力した URL の FQDN(または IP アドレス)と一致すれば、Web ブラウザはそのサーバー証明書を信頼する、という動作になっているという ことです。

- ① サーバー証明書の署名が、クライアント PC 内の「Trusted Root Certification Authorities/信頼されたルート証明機 関」に存在する認証局によって署名されていること。(←Windows の例。他 OS にも類似の仕組みが存在する。)
- ② Common Name が一致すること。(Firefox, IE11)
- ③ SAN が一致すること。(Firefox, Chrome)

ブラウザによって、サーバー証明書を信頼する条件が異なります(2018/3 現在)。

ブラウザ	Version	署名	Common Name (=Subject)	SAN	条件
Chrome	64.0.3282.186	~	無視	~	署名と、SAN が URL と一致すること。
Firefox	58.0.2	~	● (どちらか	✔ ヽが一致)	署名と、Common Name または SAN のどちらかが URL と一致すること。
IE11	11.0.9600.18860	~	~	無視	署名と、Common Name が URL と一 致すること。

[参考] 上記①は、「クライアント PC へのルート証明書をインポート(既述)」のセクションでインポートした、 「SSL-Forward-Proxy-Trust-CA」のことです。

Chrome の場合:「設定」→「詳細設定」→「証明書の管理」で表示されます。

Certificates		2						
Intended purpose: <a>								
Intermediate Certification Authorities Trusted Root Certification Au	thorities Trusted	Publ 1						
Issued To Issued By	Expiration Date	Frie *						
Security Communication Roo Security Communication R	2023/09/30	SEC						
SSL-Forward-Proxy-Trust-CA SSL-Forward-Proxy-Trust-CA	2019/02/28	<n< td=""></n<>						
Starfield Class 2 Certificatio Starfield Class 2 Certificati	2034/06/30	Sta						
thawte Primary Root CA thawte Primary Root CA	2036/07/17	tha						
Thawte Timestamping CA Thawte Timestamping CA	2021/01/01	Tha						
UTN-USERFirst-Object UTN-USERFirst-Object	2019/07/10							
VeriSign Class 3 Public Prima VeriSign Class 3 Public Prim	2036/07/17	Veri						
VeriSign Universal Root Cert VeriSign Universal Root Ce	2037/12/02	Veri 👻						
✓ []		•						
Import Export Remove	Import Export Remove Advanced							
<al></al>		ïew						
Learn more about <u>certificates</u>		Close						

次のセクションで、この現象を回避する設定を行います。

7.6.4. 「信頼されない証明書」用の認証局の生成

「信頼されない証明書」を持つサイトヘクライアント PC がアクセスした際に、必ずセキュリティ警告を出すようにする設定 方法です。

7.6.4.1. 設定

もう一つ、ルート証明書を生成します。

(1) a)「Device」 \rightarrow b)「証明書」 \rightarrow c)「生成」をクリックします。

paloalto	Dashboard ACC Mor	nitor Policies Object	s Network Device						🏝 コミット 🧉 🖓 Config 🕶 🔍 検索
			a)						3 のヘルプ
	デバイス証明書 デフォル	の信頼された証明機関							
▽□可能の整理									3個の項目s 🔿 🗙
● 証明書 D) ■ 証明書プロファイル	□ 名前	サブジェクト	発行者	CA	+-	有効期限	状態	アルゴリズム	用途
🔂 OCSP レスポンダ	SSL-Forward-Proxy-Trust-CA	CN = SSL-Forward-Proxy-Trust-CA	CN = SSL-Forward-Proxy-Trust-CA		v	Feb 28 09:43:01 2019 GMT	有効	RSA	フォワード プロキシ用の信頼された証明書
🏥 SSL/TLS サービス フロファイル 🔯 SCEP									フォワード プロキシ用の信頼されない証明書
B SSL 復号化例外	💭 🔻 🚰 dummy-CA	CN = dummy-CA	CN = dummy-CA			Mar 10 01:45:41 2019 GMT	有効	RSA	
◎応答ページ	dummy-cert01	CN = 192.168.55.11	CN = dummy-CA		✓	Mar 10 01:47:58 2019 GMT	有効	RSA	
■ ログ設定 マ ゆ サーバー プロファイル	🔲 📮 Untrust-CA	CN = Untrust-CA	CN = Untrust-CA			Mar 10 02:12:21 2019 GMT	有効	RSA	
SNMPトラップ									
🖏 Syslog 🔜 電子メール		c)							
	🔳 削除 無効化 更新 📥 インポ	ート 👼 生成 🚢 エクスポート	📥 HA キーのインポート 斗 HA キ	ーのエク	ウスポー				

(2) 以下の通り入力し、新しく認証局の証明書を生成します。

証明書名	Jntrust-CA		Untrust-CA(
共通名	Jntrust-CA		Untrust-CA(
署名者	明音に女配される 19 または	ruon 👻	
	2 認証局		認証局にチ
OCSP レスポンダ		v	
▲ 暗号設定			
アルゴリズム	RSA	-	
ビット数	2048	~	
ダイジェスト	sha256	-	
有効期限(日)	365		
正明書の属性			
タイプ	1		

(3) 生成した証明書をクリックして開きます。 a)「フォワード プロキシ用の信頼されない証明書」にチェックを入れ、b)「OK」をクリックします。



(4) 以下のように、「SSL-Forward-Proxy-Trust-CA」の用途は「フォワードプロキシ用の信頼された証明書」だけになり、 「Untrust-CA」の用途が、「フォワードプロキシ用の信頼されない証明書」になります。

名前	サブジェクト	発行者	СА	*-	有効期限	状態	アルゴ リズム	用途
SSL-Forward-Proxy-Trust-CA	CN = SSL-Forward-Proxy-Trust-CA	CN = SSL-Forward-Proxy-Trust- CA	v	V	Feb 28 09:43:01 2019 GMT	有効	RSA	フォワード プロキシ用の信頼 された証明書
▼ 🔄 dummy-CA	CN = dummy-CA	CN = dummy-CA	v		Mar 10 01:45:41 2019 GMT	有効	RSA	
aummy-cert01	CN = 192.168.55.11	CN = dummy-CA			Mar 10 01:47:58 2019 GMT	有効	RSA	
Juntrust-CA	CN = Untrust-CA	CN = Untrust-CA			Mar 10 02:12:21 2019 GMT	有効	RSA	フォワード プロキシ用の信頼 されない証明書

(5) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

7.6.4.2. 通信確認

- (1) クライアント PC の Web ブラウザから PA Firewall のマネージメントインターフェイス (<u>https://192.168.55.11</u>) ヘア クセスします。
- (2) 今度は、「保護されていません」という結果になります。
 a)「保護されていません」→ b)証明書の下の「無効」をクリックします。



(3) 「発行者/Issued by」が「Untrust-CA」となっています。

Untrust-CA は、クライアント PC にインポートしていないので、クライアント PC はこのサーバー証明書の署名検証ができないため、これを信頼しません。

Common Name(≒Subject)、SAN ともに「192.168.55.11」で、Web ブラウザの URL と一致していても、署名が検証できなければ信頼されません。

Certificate	Certificate
General Details Certification Path	General Details Certification Path
Certificate Information	Show: <all></all>
This certificate cannot be verified up to a trusted certification authority.	Field Value ^ Subject 192,158,55,11
	(a) Key Usage Digital Signature, Key Encipher (b) Enhanced Key Usage Server Authentication (1.3.6 (c) Subject Key Identifier 81 a0 24 3c 72 2f 50 ec cc c6 (c) Subject Alternative Name IP Address=192.168.55.11
Issued to: 192.168.55.11	The intervent advortion
Issued by: Untrust-CA	CN = 192.168.55.11
Valid from 2018/03/10 to 2019/03/10	
Issuer Statement	Edit Properties Copy to File Learn more about <u>certificate details</u>
ОК	ОК

- Trust ゾーンのユーザに、「セキュリティ警告は出しつつも、信頼されない証明書を持つサイトへのアクセスは許可した い」という要件の場合は、この設定を行なってください。
- 次セクションの「信頼されない証明書を持つサイトとの通信をブロック」する設定を行う場合は、この設定は必要ありません。

7.7. 信頼されない証明書を持つサイトとの通信をブロック

信頼された認証局から発行されたサーバー証明書を持たないサイトとの通信は、ブロックする設定が可能です。

- 7.7.1. 設定
- (1) a)「Objects」 \rightarrow 「復号」の下の b)「復号プロファイル」 \rightarrow c)「追加」をクリックします。

paloalto		Dashboar	d ACC	Monito	r Polici	ies Obje	ects Net	work E)evice				舎コミット	💣 🛛 👰 Config]▼ Q.検索
															S @~117
 ⊍ URL カテゴリ	٩	1 個の項目													の項目 ⋺ 🗙
▼ 図 セキュリティ プロファイル 図 アンチウイルス □ アンチフパイウェア				SSLフォワート	く プロキシ		SSL インパウ: ション	ッド インスペク	SSL プロトコル版	定			復号化なし	SSH プロキシ	
● 1000000000000000000000000000000000000		名前	場所	サーバー証明 書の確認	サポートされ ていないモー ド チェック	失敗のチェッ ク	サポートされ ていないモー ド チェック	失敗のチェッ ク	鍵交換アルゴリ ズム	プロトコル パージョン	暗号化アルゴリ ズム	認証アルゴリ ズム	サーバー証明 書の確認	サポートされ ていないモー ド チェック	失敗のチェッ ク
WildFire 分析		default	事前定義済み						RSA	最小パージョ ン: TLSv1.0	トリプル DES 暗 号化	SHA1			
☆ データ フィルタリング ■ DoS プロテクション	4								DHE	最大パージョ ン: Max	RC4	SHA256			
 図 セキュリティ プロファイル ク ■ ログ転送 									ECDHE		AES128-CBC AES256-CBC	SHA384			
											AES128-GCM				
		c)									AES256-GCM				
	ŧ	追加 日前時	: 💿 ⊐ ピー 🖪	PDF/CSV											

 (2) a)名前に「Decrypt_Profile01 (任意)」と入力します。
 b)「SSL 復号化」タブ → c)「SSL フォワードプロキシ」タブの、「サーバー証明書の確認」内にある d)「発行者が信頼 されていないセッションをブロック」にチェックをいれます。e)「OK」をクリックします。

復号プロファイル	0
b) お Decrypt-Profile01 a) SSL復号化 復号化なし SSH プロキシ	
C) SSL フォウート フロキシ SSL コンパウント インスペクション サーパー証明書の確認 I 期限切れ証明書のセッションをブロック ダーパー証明書の状態が不明なセッションをブロック (1) 証明書の状態が不明なセッションをブロック (2) 証明書の状態がタイムアウトのセッションをブロック 証明書の延長を制限 詳細 証明書の延長を利限 詳細 証明書のゴモンネーム (CN) 値を SAN 拡張項目に追加	SSL ノロトコル設定 サポートされていないモード チェック サポートされていないパージョンのセッションをブロック 協号スイートがサポートされていないセッションをブロック クライアント認証を使用するセッションをブロック ケライアント認証を使用するセッションをブロック リソースを使用できない場合にセッションをブロック HSM を使用できない場合にセッションをプロック
注: サポートされていないモードおよび失敗については、セッション情報が 12 時間キャッシュされます。こ するには、チェック ポックスをオンにしてください。	のため、同じホストとサーバー ペア間の以降のセッションは復号化されません。 これらのセッションをブロック

(3) a)「Policies」 \rightarrow b)「復号」で表示された「Dec_Rule1」行の、復号プロファイル列の c)「なし」をクリックします。

Dashboard ACC						Polici	es Ob	jects	Network	Device			
■ セキュリティ	۹.					<u>a)</u>							
∄> NAT ♣ QoS					送信元		5	先				復号オプショ	y
 ・ボリシー ベース フォワーディン・ ・ ・ ・	1	名前 Dec_Rule1	タグ none	ゾーン (知) Trust	アドレス any	ユーザー any	ゾーン päij Untrust	アドレス any	URL カテゴリ any	サーピス any	アクション decrypt	タイプ ssl-forward-proxy	復号プロファイル なし C)

(4) a)復号プロファイルで「Decrypt-Profile001」を選択し、b)「OK」をクリックします。

復号オプション			0
アクション	○ 復号なし ● 復号		
タイプ	SSL フォワード プロキシ	~	
復号プロファイル	Decrypt-Profile01	a)	~
	b)	ОК	キャンセル

(5) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

7.7.2. 動作確認

- Trust ゾーン: 192.168.45.0/24 のクライアント PC の Web ブラウザ(例: Chrome)で、PA Firewall のマネージメントインターフェイス (<u>https://192.168.55.11</u>) ヘアクセスします。
- (2) 以下のような、ブロックされたことを示す画面が表示されます。

Certificate Error X	
	☆ :
Certificate Error	
There is an issue with the SSL certificate of the server you are trying to contact.	
Certificate Name:	
IP: 192.168.55.11	
Category: private-ip-addresses	
Issuer:	
Status: untrusted	
Reason:	
User: 192.168.45.32	

7.8. [参考] そもそも「信頼された証明書」や「信頼されない証明書」とは?

PA Firewall は、信頼された認証局(証明機関)のリストを事前に保持しています。

(Windows 等のクライアント PC の Web ブラウザが事前に保持している「Trusted Root Certificate Authorities/信頼され たルート証明機関」のリストと同等だと考えれば分かりやすいかもしれません。)

インターネット上に存在する Web サイトが持つサーバー証明書が、そのリストに存在する認証局が発行したものであれ ば、「信頼された証明書」であると判断し、逆にそのリストにない認証局が発行した証明書であれば、「信頼されない証明書」 である、と判断します。

その認証局のリストは、a)「Device」 \rightarrow b)「証明書」 \rightarrow c)「デフォルトの信頼された証明機関」で確認できます。

paloalto	Dashboard ACC Monitor	Policies Objects Netwo	rk Device		🛎 コミット 🧉 闷 Config 🕶 🔍 検索
			a)		😋 🔞 ヘルプ
 	デバイス証明書 デフォルトの信	類された証明機関 2)			
2回 設定監査					246 個の項目s 🕂 🗶
5 管理者	□ 名前	サブジェクト	発行者	有効期限	状態
 管理者ロール 認証プロファイル 	GeoTrust_Primary_Certification_Authority	GeoTrust Primary Certification Authority - G2	GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	有効
認証シーケンス 国 ユーザー ID	GeoTrust_Primary_Certification_Authority	GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Authority - G3	Dec 1 23:59:59 2037 GMT	有効
WM 情報ソース	GeoTrust_Universal_CA	GeoTrust Universal CA	GeoTrust Universal CA	Mar 4 05:00:00 2029 GMT	有効
▼ 2000年の修理 ■ 証明書 b)	GeoTrust_Universal_CA_2	GeoTrust Universal CA 2	GeoTrust Universal CA 2	Mar 4 05:00:00 2029 GMT	有効
9月 証明者ノロノアイル	GlobalSign b	GlobalSign	GlobalSign	Jan 19 03:14:07 2038 GMT	有効
🐼 OCSP レスボンダ 🔒 SSL/TLS サービス プロファイル	🔲 📮 GlobalSign c	GlobalSign	GlobalSign	Jan 19 03:14:07 2038 GMT	有効
SCEP	GlobalSign_Root_CA	GlobalSign Root CA	GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	有効
□ SSL 復号化例外 ■ SSL 復号化例外	GlobalSign_Root_CAR2	GlobalSign	GlobalSign	Dec 15 08:00:00 2021 GMT	有効
「日」ログ設定	GlobalSign_Root_CAR3	GlobalSign	GlobalSign	Mar 18 10:00:00 2029 GMT	有効
▼ 1 サーバー プロファイル ■ SNMP トラップ	Global_Chambersign_Root2008	Global Chambersign Root - 2008	Global Chambersign Root - 2008	Jul 31 12:31:40 2038 GMT	有効
Syslog 副 電子メール	Go_Daddy_Root_Certificate_Authority	Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	有効
HTTP Netflow	Government Root Certification Authority	/C=TW/O=Government Root Certification Authority	/C=TW/O=Government Root Certification Authority	Dec 31 15:59:59 2037 GMT	有効
RADIUS	ちかん 気かん たてカフポート	Hollonia Acadomic and Docoarch	Hollonic Academic and Recearch	Dec 1 12:40:52 2021 CMT	本か

7.9. 一部の URL カテゴリを復号化から除外する

PA Firewall は、URL カテゴリ単位に SSL 復号化を実施する/しないの制御が可能です。

ここでは、「ユーザーのプライバシー保護の観点から、インターネットバンキングなどの金融系の復号化は行わない」という 要件を想定し、その設定を行います。

7.9.1. 金融サービスのカテゴリは復号化から除外する設定

(1) a)「Policies」 \rightarrow b)「復号」 \rightarrow c)「追加」をクリックします。

-III paloalto	Da	ashboard	ACO		Ionitor	Policies	Objects	s Netv	vork Devi	ce			å⊐≥
					L								
B⇒ NAT	٩.												
⁶⁶ QoS ⁶⁶ ポリシー ベース フォワーディング					送信元		宛	洗			復号オプション		
復号 b)		名前	タグ	ゾーン	アドレス	ユーザー	ゾーン	アドレス	URL カテゴリ	サービス	アクション	タイプ	復号プロファイル
○ トンネル検査 ■ アプリケーション オーバーライド ● ロッエ	1	Dec_Rule1	none	(22) Trust	any	any	🕅 Untrust	any	any	any	decrypt	ssl-forward-proxy	Decrypt-Profile01
るが認証 ● DoS プロテクション	C		2 👩 ר	ピー 🗖 倉	动化 🗨 🗮	动化 移動			ちていない!!	リカ没想すこ		トカウンターのリ	7 W N -
	-		r 💟 –	C- 🕑 18		3016 1990 -		◎ 一便用る	ri (11211)1-	ルの強調表示		F 3029-00	evr •

(2) a)「全般」タブで、b)名前に「Finance (任意)」と入力します。

復号ポ	リシール	ール				0
全般	送信元	宛先	サービス/URL カテゴリ	オプション		
<u> </u>	名前	Finance	b			
	内容					
	タグ					~
					OK	キャンセル

(3) a)「送信元」タブで、b)「追加」をクリックし、c)「Trust」を選択します。

復号ポ	リシール・	ール					Q
全般	送信元	宛先	サービス	ス/URL カテゴリ	オプション		
🔲 W3	。 <i>さ</i> れか			🗹 いずれか		any	~
□ 送	言元ゾーン ▲	<u></u>		🔲 送信元アドレス		🔲 送信元ユーザー	A
1	Trust	C)					
<u> </u>	_						
b) ₽ 追カ	□■削除			● 追加 ■ 削除		● 追加 ■ 削除	_
		_	_	Negate			
						D	K キャンセル

(4) a)「宛先」タブで、b)「追加」をクリックし、c)「Untrust」を選択します。

復号ポ	リシール・	ール			0
全般	送信元	宛先 a)	サービス/URL カテゴリ	オプション	
<u>ו</u> ואז	ずれか			🗹 いずれか	
- 宛:	先ゾーン ▲			🔲 宛先アドレ	⊼ ▲
∑ (pa	Untrust	C)			
	-				
b)					194
					194
				Negate	
					OK キャンセル

(5) a)「サービス/URL カテゴリ」で、URL カテゴリの b)「追加」をクリックし、c)「financial-services」を選択します。
 (※URL フィルタリングのサブスクリプションライセンスが必要です。)

復号ポリシー ルール	0
全般 送信元 宛先 サービス/URL カテゴリ a)	オプション
any	🔲 いずれか
■ サービス ▲	🔲 URL カテゴリ 🔺
	✓ financial-services C)
	b)
●追加 ● 削除	+ 追加 ●削除
	OKキャンセル

(6) a)「オプション」タブで、b)アクションで「復号なし」を選択し、c)タイプが「SSL フォワードプロキシ」であることを確認しま す。d)「OK」をクリックします。

復号ポ	リシール・	ール				0
全般	送信元	宛先	サービス/URL カテゴリ	オプション		
b)	アクション(● 復号な	し ② 復号	a)		
	タイプ	SSLフォワ	フード プロキシ		C)	~
復号フ	プロファイル	None				~
					d) ok	キャンセル

(7) a)「Finance」が選ばれた状態で、b)「移動」をクリックし、c)「上へ」をクリックします。

paloalto	Da	ashboard	AC	C N	<i>l</i> onitor	Policies	Object	s Netw	vork Devid	e			총 그 3
セキュリティ													
⇒ NAT ▲ QoS					送信元		Ŕ	洗				復号オプショ	2
🖫 ポリシー ベース フォワーディング		名前	タグ	ゾーン	アドレス	ユーザー	ゾーン	アドレス	URL カテゴリ	サービス	アクション	タイプ	復号プロファイル
◎ 復号	1	Dec Rule1	none	fiii) Trust	any	any	(22) Untrust	any	any	any	decrypt	ssl-forward-proxy	Decrypt-Profile01
(塗)トンネル検査 国 マブリケーション オーバーライド	2	Finance	none	(22) Trust	any	any	🚧 Untrust	any	financial-services	any	no-decrypt	ssl-forward-proxy	なし a)
	4					王	上部へ	_					
使 DoS プロテクション						🛨 🗄	:^ (:)					
						T 💽	\$	4					
						- H	下部へ						
	÷	追加 🖃 削	除 👩 🏾	ピー 🖌 🧃	「効化 💿 無	効化 移動 -	b) 🛓 PDF/CS	₩ 🔲 使用さ	れていないルーノ	レの強調表示	ールヒッ	ット カウンターのリ	セット・

(8) 「Finance」が上へ移動した状態です。

paloalto	Da	ashboard	ACC) N	Ionitor	Policies	Objects	s Netw	vork Devid	e			🏝 🏼 🗉
<u>⇔</u> セキュリティ	٩.												
≌≫ NAT As OoS					送信元								ン
🐻 ポリシー ベース フォワーディング		名前	タグ	ゾーン	アドレス	ユーザー	ゾーン	アドレス	URL カテゴリ	サービス	アクション	タイプ	復号プロファイル
	1	Finance	none	(22) Trust	any	any	(22) Untrust	any	financial-services	any	no-decrypt	ssl-forward-proxy	なし
トンネル検査 アプリケーション オーバーライド	2	Dec_Rule1	none	🕅 Trust	any	any	🚧 Untrust	any	any	any	decrypt	ssl-forward-proxy	Decrypt-Profile01
象 認証 優 DoS プロテクション	•	追加 🕒 削隊		Ľ– ₽ 4	动化 同無	· 动化 移動 -		∨ ■ 使田→	・カブいかいルート	しの公理書示	│ ルール ヒッ	トカウンターのリ	セット •

- (9) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (10) 今一度、「Device」→「ライセンス」で、「PAN-DB URL Filtering」のダウンロード状態が「Finished Successfully」であることを確認します。(これが空の状態だと期待する動作になりません。)

PAN-DB URL Filtering	
発行日	February 02, 2018
有効期限	February 02, 2019
内容	Palo Alto Networks URL Filtering License
アクティブ	はい
ダウンロードの状態	2018-02-20 09:55:07 PAN-DB download Finished successfully. 再ダウンロード

7.9.2. 通信確認

SSL/TLS 復号化の設定が、期待通り動作する(金融系サービスだけが復号化されない)ことを確認します。

7.9.2.1. 金融系サービスへアクセス

(1) ある銀行の HTTPS サイトへアクセスします。
 a)の鍵マークのある部分をクリックし、b)証明書の下の「有効」をクリックします。



(2) Issued by / 発行者が、PA Firewall で生成した認証局(SSL-Forward-Proxy-Trust-CA)ではない(=復号化されていない)ことがわかります。

Certificate	X
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	
Ensures the identity of a remote computer Proves your identity to a remote computer 1.3.6.1.4.1.6334.1.100.1	
* Refer to the certification authority's statement for details.	_
Issued by: Cybertrust Japan EV CA G2	
Valid from 2017/ 12/ 18 to 2018/ 12/ 31	
Learn more about tertificates	nt
Of	

7.9.2.2. 金融系以外の Web サイトヘアクセス

(1) 金融系以外の Web サイト(例: https://www.paloaltonetworks.com)へアクセスします。
 a)の鍵マークのある部分をクリックし、b)証明書の下の「有効」をクリックします。

What's New in PAN-OS 8 ×			
← → (a) ● 保護された通信 https://www.paloaltonetwork	ks.com/products/new/new-panos8-1		☆ :
保護された接続 × 保護された接続 * お客様がこのサイトに送信した情報 パスワード、クレジットカード番号など)が第三者に見られることはありません。詳しく見る	Log in » Get Support	Q	MENU
♣ Flash 確認(デフォルト) マ			
■ 証明書 b) 有効 ◆ Cookie 160 個が使用中 サイトの設定	v 8.1		
A wealth of innovations to secure cloud	ds, networks and		

(2) Issued by / 発行者が、PA Firewall で生成した認証局(SSL-Forward-Proxy-Trust-CA)となっています=復号化されています。

Certificate	×
General Details Certification Path	
Certificate Information	-
This certificate is intended for the following purpose(s):	
Ensures the identity of a remote computer Proves your identity to a remote computer	
· · · · · · · · · · · · · · · · · · ·	
Issued to: *.paloaltonetworks.com	
Issued by: SSL-Forward-Proxy-Trust-CA	
Valid from 2017/ 07/ 11 to 2018/ 10/ 11	
Learn more about <u>certificates</u>	
ОК	

8. コンフィグの操作

PA Firewall は、実施したコンフィグレーションをスナップショットとして保存しておくことができます。 そのスナップショットをロードすることで、その時実施したコンフィグレーションまで戻ることができます。

8.1. スナップショットの保存

ここまで実施したコンフィグをスナップショットとして保存しておきます。

(1) a)「Device」→ b)「セットアップ」→ c)「操作」→
 「設定の管理」の中の、d)「名前付き 設定スナップショットの保存」をクリックします。



(2) a)任意のファイル名を入力して、b)「OK」をクリックします。



(3) 「閉じる」をクリックします。保存完了です。



8.2. スナップショットのエクスポートとインポート

スナップショット(XML 形式ファイル)を外部に保存することができ、再度それをインポートすることができます。

- 8.2.1. エクスポート
- (1) 「名前付き 設定スナップショットのエクスポート」をクリックします。



(2) a)エクスポートしたいファイルを選択して、b)「OK」をクリックし、保存先を指定します。



8.2.2. インポート

外部保存しておいたスナップショットを、インポートします。

(1) 「名前付き 設定スナップショットのインポート」をクリックします。



(2) a)「参照」をクリックして、外部保存しておいたファイルを指定し、b)「OK」をクリックします。

名前付き 設定のイ	ンポート		0 🗵
ファイルのインポート		_{参照} a)	
	b)	(t. r	
	~/ OK	++	シセル

8.3. スナップショットのロード

スナップショットをロードすることで、スナップショットを取得した時点のコンフィグまで戻すことができます。

(1) 「名前付き 設定スナップショットのロード」をクリックします。

naloalto											
	Dashboard	ACC	Monitor	Policies	Objects	Network	Device				
↓ セットアップ ● 点可用性	管理 操作	サービス	インターフ	ェイス テ	レメトリー	コンテンツID	WildFire	セッション HSM			
□ 同う///注 ■ 設定監査	設定の管理						デバー	イスの操作			
8 管理者	戻す	最後に保存し	た 設定に戻します	r -			ड ी <i>ने</i> /	パイス の再起動			
② 管理者ロール ③ 認証プロファイル 3	保存	実行中の 設定 名前付き 設定	に戻します スナップショット	の保存			೯ ೦ ಕ್	∈⊚ デバイス のシャットダウン			
※ 認証シーケンス 国 ユーザー ID の ロージー ID	□-ド	保護 設定の存 名前付き 設定	を スナップショット	のロード]					
 WM 情報ソース ▼ ▼ ○ 証明書の管理 	エクスポート	設定バージョ 名前付き 設定	ンのロード ミスナップショット	・のエクスポート		-	その	他			
🗐 証明書 🗐 証明書プロファイル		設定パージョ デバイス状態	ンのエクスポート のエクスポート				した (別) (別) SN	スタム ロゴ MP のセットアップ			
₩ OCSP レスポンダ B SSL/TLS サービス プロファイ 「」 SCEP	インポート	名前付き 設定 デバイス状態	ミスナップショット のインポート	ーのインポート							

(2) a)保存しておいたスナップショットを選択し、b)「OK」をクリックします。

名前付き設定	ピのロード			0
名前	PA-CONFIG_20180324		a)	-
復号キー	••			
		b)	ок	キャンセル

(3) 「閉じる」をクリックします。 ロードが完了し、その時点までのコンフィグに戻っています。

Config loaded from PA-CONFIG 20180324

Trust ゾーンから Untrust ゾーン方向(インターネット方向)への通信ができることを確認したので、Firewall のマネージメントインターフェイスを Trust ゾーンに接続して、PA Firewall の保護対象に変更します。

9.1. 変更後のネットワーク構成



PA Firewall のマネージメントインターフェイスの IP アドレスを、192.168.45.11、デフォルトゲートウェイを 192.168.45.20 に変更し、Trust ゾーン側のネットワークに接続し直します。

9.2. マネージメントインターフェイスの設定変更

(1) a)「Device」 \rightarrow b)「セットアップ」 \rightarrow c)「インターフェイス」で表示された d)「Management」をクリックします。

naloalto											
NETWORKS®	Dashboard	ACC	Monitor Policies		Objects	jects Network De		e			ミット 🧉 闷 Config 🕶 🔍 検索
											S 💿 へル
セットアップ b) 日の用作	管理 操作	サービス	インター	;) -フェイス	テレメトリー	コンテンツ	UD Wi	ildFire	セッション	HSM	
2 設定監査	インターフェイス	名	有效		速度			IPアド	レス		サービスが有効
ペマンスワード プロファイル の 管理者 の 管理者 の 管理者ロール	Management	d)			auto-ne	gotiate		192.16	8.55.11		Ping,HTTPS,SSH

(2) ネットワーク構成に従って a)IP アドレスを「192.168.45.11」、b)デフォルトゲートウェイを「192.168.45.20」に変更します。c)「OK」をクリックします。

管理インターフェイス	設定	0
IP タイプ	 ③ スタティッ ○ DHCP クライアン ク ト アクセス許可 IP アドレス 	
IP アドレス	192.168.45.11 a)	1
ネットマスク デフォルト ゲートウェイ	192.168.45.20 b)	
IPv6 アドレス/プレフィックス の長さ		
デフォルト IPv6 ゲートウェイ		
速度	auto-negotiate 💌	
MTU	1500	
ネットワーク接続性サービス	ζ	
HTTP	HTTP OCSP	
HTTPS	Telnet	
SSH	✓ Ping	
SNMP	ID	
ニューザー ID Syslog リン	スナー 🗌 ユーザー ID Syslog リスナー	
SSL	UDP 单追加 ● 削除	
		2

- (3) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (4) コミット処理を実施することで、マネージメントインターフェイスの IP アドレス変更が反映されるので、現在の WebUI のアクセス先 IP アドレスではなくなるため、Commit の状態は 100%になる前に止まりますが、問題ありません。

Commit の状!	態	0
操作	コミット	
状態	アクティブ	
結果	保留	
進捗	98%	
詳細		
警告		
	<u>م باللا</u>	

- (5) マネージメントインターフェイスを Untrust ゾーンから物理的に切断し、Trust ゾーンへ接続します。
- (6) Web ブラウザで、<u>https://192.168.45.11</u> へ接続し、WebUI が応答することを確認します。

マネージメントインターフェイスのアドレス変更を行っただけでは、「ダイナミック更新」や「ソフトウェア」の「今すぐチェック」 を実行すると、以下のエラーに遭遇します。

NETWORKS ¹	Dashboard	AGC Mon	Htor Policies Obje	ects Network	Device		@ _ < y	
					a)			
ナーバー プロファイル	۹.							
Syslog	パージョン	サイズ	リリース日	使用可能	現在インストール済み	アクション		
電子メール	8.0.8	431 MB	2018/02/11 09:42:06			ダウンロード	リリース ノート	
🗟 НТТР	8.0.7	431 MB	2017/12/28 10:26:05	Downloaded	v	再インストール	リリース ノート	
Netflow	8.0.6	431 MB	2017/11/13 22:44:23			ダウンロード	リリース ノート	
RADIUS	8.0.6-h3					$\nu \Box + K$	リリース ノート	
TACACS+	8.0.5	17-				ストール	リリース ノート	
LDAP	8.0.4	Failed to check	upgrade info due to generic co	mmunication error. Ple	ase check network connectivity	y and y 🖂 🕂 🖂	リリース ノート	
Kerberos	8.0.3	try again.				VD-K	リリース ノート	
SAML アイナンティティ ノ マルギ フックター初訴	8.0.3-h4					20-K	リリース ノート	
コーカル フーザー データベー	8.0.2					20-F	リリース ノート	
ユーザー	8.0.1			閉じる		×0-k	リリース ノート	
ユーザー グループ	8.0.0					トール	リリース ノート	
レクジュール設定されたログ(7.1.15	301 MB	2018/01/17 15:57:51			ダウンロード	リリース ノート	
(フトウェア b)	7.1.14	300 MB	2017/11/21 18:50:37			ダウンロード	リリース ノート	
IDDAIPTOLECL 9 94 99 1	7.1.13	297 MB	2017/10/12 14:41:53			ダウンロード	リリース ノート	
イナミック更新	7.1.12	297 MB	2017/08/30 06:39:18			ダウンロード	リリース ノート	
ライセンス	7.1.11	297 MB	2017/07/06 15:36:57			ダウンロード	リリース ノート	
ナポート	7.1.10	297 MB	2017/05/22 17:27:56			ダウンロード	リリース ノート	

(M:a)「Device」 \rightarrow b)「ソフトウェア」 \rightarrow c)「今すぐチェック」の場合

これは、デフォルトでは、マネージメントインターフェイスが <u>https://updates.paloaltonetworks.com</u> ヘアクセスする際、「信頼された認証局から発行された証明書のときだけ接続する」という動作になっているからです。

この状態を回避する策を3つ紹介します。

9.3.1. <方法 1>「更新サーバーID の確認」チェックを無効化する

ーつめの方法は、a)「Device」 \rightarrow b)「セットアップ」 \rightarrow c)「サービス」で表示された、d)「更新サーバーID の確認」のチェックを外すことです。

このチェックが入っていることで、updates.paloaltonetworks.comのサーバー証明書が信頼された認証局から発行されたものである場合にだけ接続する、というモードになっています。

(1) e) 🔯 をクリックします。

m paloalto									
NETWORKS®	Dashboard	ACC	Monitor	Policies	Objects	Network	Device		
🤯 セットアップ b)	管理操作	+-EZ	インター	フェイス	テレメトリー	コンテンツ	D WildFire	セッション	HSM
高可用性								1	
	サービス					* e	•)		
			更新サーバー	undates naloalte	onetworks.com		_		
		更新サー	ベー ID の確認						
総認証プロファイル			DNS	₩_,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,					
2 認証シーケンス		プライマリ	DNS サーバー	192.168.55.2					
■ ユーザー ID		セカンダリ	DNS サーバー	4.2.2.2					
🚇 VM 情報ソース		FQDN	更新時間(秒)	1800					
▼ 뎙 証明書の管理			Proxy Server						
፼ 証明書	プラ・	イマリ NTP サー	バー アドレス	ntp.nict.jp					
📮 証明書プロファイル	プライ	マリ NTP サー/	《一認証タイプ	None					
OCSP レスポンダ	セカ	ンダリ NTP サー	バー アドレス						
₿ SSL/TLS サービス プロファイ									
SCEP	サービス機能								
E SSL 復号化例外									
	1 - EX 11-1	C U BRAE							

- (2) 表示された画面で、「更新サーバーID の確認」のチェックを外し、「OK」をクリックします。
- (3) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (4) a)「Device」 \rightarrow b)「ソフトウェア」 \rightarrow c)「今すぐチェック」でエラーが出なくなったことを確認してください。

9.3.2. <方法 2> updates.paloaltonetworks.com を「SSL 復号化例外」に入れる

二つめの方法は、a)「Device」 → 証明書の管理の下の b)「SSL 復号化例外」に、updates.paloaltonetworks.com を追加することです。

このことで、この宛先に関しては SSL 復号化が行われなくなるので、その Web サイトが持つ、本来のサーバー証明書がマネージメントインターフェイスにそのまま到達するようになるからです。

結果、この方法使うと、暗号化されたままとなるため、PA Firewall は通信内容を検査することはできなくなります。

(1) c)「追加」をクリックします。

paloalto	Dashboard ACC	Monitor Policies Objects I	Network Device	🏝 コミット 🧉 阔 Cơ	onfig - 9、検索
			a)		ら ③ヘルプ
🔒 認証プロファイル	۹.			138	;個の項目s → 🗙
22 認証シーケンス ■2 フーザー ID	□ ホスト名	場所	内容	復号化からの除外	
型 VM 情報ソース	*.whatsapp.net	事前定義済み	whatsapp: pinned-cert		
▽ 🔓 証明書の管理	kdc.uas.aol.com	事前定義済み	aim: client-cert-auth		
፼ 証明書	bos.oscar.aol.com	事前定義済み	aim: client-cert-auth		
🔁 証明書プロファイル	*.agni.lindenlab.com	事前定義済み	second-life: client-cert-auth		
🐺 OCSP レスポンダ	*.onepagecrm.com	事前定義済み	onepagecrm: pinned-cert		
🔓 SSL/TLS サービス プロフェ	update.microsoft.com	事前定義済み	ms-update: client-cert-auth		
CCED	*.update.microsoft.com	事前定義済み	ms-update: client-cert-auth		
🚨 SSL 復号化例外 🛛 🗋	activation.sls.microsoft.com	事前定義済み	ms-product-activation: client-cert-auth		
の応答ページ	Yuuguu.com	事前定義済み	yuuguu: client-cert-auth		
1000000000000000000000000000000000000	yuuguu.com	事前定義済み	yuuguu: client-cert-auth		
▼40 サーバー プロファイル	Pac etiX VPN	事前定義済み	packetix-vpn: client-cert-auth		
SNMP トラップ	C. Sof Ether VPN	事前定義済み	packetix-vpn: client-cert-auth		
Syslog	🕂 追加 🖃 削除 💿 コピー 🕑 4	「効化 🐻 無効化 🔜 廃止された機能を表示 除外	された共通名および SNI		

(2) a)ホスト名に「updates.paloaltonetworks.com」、b)「除外」にチェックをいれ、c)「OK」をクリックします。



- (3) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (4) a)「Device」 \rightarrow b)「ソフトウェア」 \rightarrow c)「今すぐチェック」でエラーが出なくなったことを確認してください。

9.3.3. <方法 3> PA Firewall で生成したルート証明書を「信頼されたルート CA」にする

三つめの方法は、PA Firewall で生成したルート証明書を、マネージメントインターフェイスが信頼できるようにすることです。

通信エラーメッセージは、PA Firewall から発行される「SSL-Forward-Proxy-CA」証明書を、マネージメントインターフェイスが信頼できないことで発生しているためです。

(1) a)「Device」→ 証明書の管理の下の b)「証明書」で表示された c)「SSL-Forward-Proxy-Trust-CA」をクリックしま す。

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	1					📥 コミット 💣 🍃	Config ▼
														😋 🕢 ヘルプ
QVM 情報ソース	デバイス	正明書 デフ	7ォルトの信頼	頼された証明機	観									
· 証明書 b)	Q													1個の項目 → 🗶
●目証明書フロファイル ↓ OCSP レスポンダ	🗌 名前		サブ	゚ジェクト		発行者		СА	*-	有効期限	状態	アルゴリ ズム	用途	
SCEP	🔲 👼 SS	L-Forward-Proxy-	Trust-CA C	= SSL-Forward-Pro>	ky-Trust-CA	CN = SSL-Forward-P	roxy-Trust-CA	•		Feb 28 09:43:01 2019 GMT	有効	RSA	フォワード プロキシ用の	信頼された証明書
◎ SSL 復号化例外													フォワード プロキシ用の	信頼されない証明書
 ○ ○<td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td>														

(2) a)「信頼されたルート CA」にチェックを入れて、b)「OK」をクリックします。

名前	SSL-Forward-Proxy-Trust-CA	
サブジェクト	/CN=SSL-Forward-Proxy-Trust-CA	
発行者	/CN=SSL-Forward-Proxy-Trust-CA	
発効日時	Feb 28 09:43:01 2018 GMT	
有効期限	Feb 28 09:43:01 2019 GMT	
アルゴリズム	RSA	
	☑ 認証局	
	☑ フォワード プロキシ用の信頼された証明書	
	✓ フォワード プロキシ用の信頼されない証明書	
_	▼ 信頼されたルート (A _ 2)	

- (3) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (4) a)「Device」 \rightarrow b)「ソフトウェア」 \rightarrow c)「今すぐチェック」でエラーが出なくなったことを確認してください。

それぞれの方法で一長一短ありますが、<方法 2>を推奨します。

<方法 2>は、更新サーバー(updates.paloaltonetworks.com)のサーバー証明書が正しいものであることを確認できる一方で、SSL/TLS 復号は行われません。

しかし、復号化しないことで PA Firewall の負荷軽減にもなるので、特に更新サーバーへの復号化を必要としない限りは、 そのサーバーが正しいものであることの確認はできているので、<方法 2>で良いと思います。 10. サービスを限定するポリシーの設定

ここまでのポリシー設定では、全てが許可された状態になっています。

このセクションでは、Trust ゾーンから Untrust ゾーン方向(インターネット方向)の通信を、 HTTP (TCP/80) と HTTPS (TCP/443)のみ許可する、という方針を想定し、ポリシーを変更します。

この TCP や UDP 等のプロトコルとポート番号の組合せを、「サービス」と呼びます。

10.1.HTTPとHTTPSのみ許可する設定

10.1.1. HTTP(TCP/80)サービスの追加

PA Firewall がデフォルトで持つサービスは、以下の2つです。

- service-http: TCP/80, 8080
- service-https: TCP/443

HTTPとHTTPS(TCP/80, TCP/443)サービスのみ許可したいので、service-https はそのまま利用できますが、servicehttp が持つ 8080 は不要です。よって、TCP/80 だけを許可する新しいサービスを定義することにします。

(1) a)「Objects」 \rightarrow b)「サービス」 \rightarrow c)「追加」をクリックします。



(2) a)名前に「http(任意)」、b)プロトコルは「TCP」を選択、c)宛先ポートに「80」を入力し、d)「OK」をクリックします。

サービス	0
名前	http a)
内容	
プロトコル	TCP UDP SCTP Association Activity b)
宛先ポート	80 C)
送信元ポート	[>= 0]
	ポートには、単一のポート番号、範囲 (1 ~ 65535)、またはカンマ区切りの値 (80, 8080, 443) を指定できます
セッション タイム	● アプリケーションから継承 ○ オーバーライド
5.51	
タヴ	· ·
	d) _{OK} キャンセル

10.1.2. ポリシーの設定

HTTP(TCP/80)とHTTPS(TCP/443)のみ許可するポリシーを設定します。

(1) a)「Policies」 \rightarrow b)「セキュリティ」 \rightarrow c)「追加」をクリックします。

		Dashboard AC		Monitor	Policie	s Obj	ects I	Vetwork Devi	се				📥 コミッ	ト 🗗 😡 Config]▼ Q 検索
															😋 💿 ヘルプ
■ セキュリティ b)	٩													2個0	D項目s 🔿 🗙
SP NAT							送信元			吃先					
● ボリシー ベース フォワーディング ● 復号 ▲ トンタル検索		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	allow outbound	none	universal	🕅 Trust	any	any	any	🕅 Untrust	any	any	any	📀 許可	none	
 ドンネル検査 アプリケーション オーバーライド 	2	intrazone-default 🧇	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
🍃 認証	< 3	interzone-default 🔮	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none
€DoS プロテクション	Ĩ.														
		<u>,</u>													
	0	c)													
_	÷	追加 🖃 削除 💿 コピ	- 🎕 オ	ーバーライト	: * 戻す	✔ 有効化	💿 無効化	移動 - 📄 使用され	れていないル	ールの強調表	沶				

(2) a)「全般」 → b)名前に「allow outbound web (任意)」と入力します。

セキュ	リティポ	リシールーノ	٢				0
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	
<u>u</u>)	名前	allow outbound	web	o)			
ル	ール タイプ	universal (defau	lt)				~
	内容						
	タグ						-
						OK キャン	セル

(3) a)「送信元」→ b)「追加」→c)「Trust」を選択します。

セキュリティ ポリシー ルール									
全般	送信元	ユーザー	宛先	アプリケーシ	'ヨン	サービス/URL カテコ	עב	アクション	
いずれか						🗹 いずれか			
□ 送信元ゾーン ▲						📓 送信元アドレス 🔺			
L [10]	Trust	b)							
b)									
🕂 追加	□ ■ 削除				🕂 追加	a 🕒 1111k			
					Nega	ate			
18								***	ŧル

(4) a)「宛先」→ b)「追加」→c)「Untrust」を選択します。



(5) 「アプリケーション」は、デフォルトの「いずれか」のままにします。



(6) a)「サービス/URL カテゴリ」 → b)「追加」 →c)設定した「http」と「service-https」を選択します。

セキュ	リティポリ	ノシールーノ	L					0
全般	送信元	ユーザー	宛先	アプリケーシ	эν	サービス/URLカテゴリ a)	アクション	
選択		-			🗹 ហរ្វ	「わか	•	
サ・	-ピス ▲				UR	L カテゴリ 🔺		
×	http		C	;)				
2 ×	service-https							
	-							
D)					-			-
+ 3	1 - 削除				+追加			
						-		-
							OK ++>>t	216

(7) a)「アクション」で、b)が「Allow」であることを確認します。
 c)「OK」をクリックします。


10.1.3. 全許可ポリシーの削除

全許可ポリシーである、allow outbound を削除します。

(1) a)「allow outbound」が選択された状態で、b)「削除」をクリックします。

paloalto		Dashboard ACC		Monitor	Policie	es Obj	ects I	Vetwork Devi	ce				🍐 コミッ	ト 💣 퉪 Confiç	」▼ ♀ 検索
															ら ③ヘルプ
セキュリティ	٩													3個0	D項目s 🗙
Strain NAT							送信元		3	记先					
🗟 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
當復号 ▲ トンネル検査	1	allow outbound	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	any	📀 許可	none	🖻 a)
 □ アプリケーション オーバーライド ☆ 認証 	2	allow outbound web	none	universal	🕅 Trust	any	any	any	(22) Untrust	any	any	http k service-https	🕑 許可	none	
(€DoS プロテクション	3	intrazone-default 🥹	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
	4	interzone-default 🧇	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none
		b)													
	+;	追加 🖃 削除 💿 コピー				✔ 有効化	◎ 無効化	移動 - 📃 使用され	れていないル	ールの強調表	示				

(2) 「はい」をクリックします。

セキュ	リティ ルール
?	1 個 の「セキュリティ ルール」の エントリ を削除 しますか?

(3) 以下は、「allow outbound」が削除され、「allow outbound web」とデフォルトのポリシーだけになった状態です。

paloalto		Dashboard ACC		Monitor	Policie	s Obj	ects N	letwork Devi	се				🏝 コミッ	⊢ 💣 📢 Config	- ♀検索
															ら ③ヘルプ
📟 セキュリティ	٩													3個0	D項目s 🛃 🗶
₩ NAT							送信元		3	8先					
💀 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
び 復号 ふ トンネル検査 マブリケーション オーバーライド	1	allow outbound web	none	universal	🕅 Trust	any	any	any	🎮 Untrust	any	any	http service-https	🕑 許可	none	
■ アクリアーション オーバー シード 参 認証	< 2	intrazone-default 😔	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可	none	none
(€DoS プロテクション	3	interzone-default 🔮	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none
	÷	追加 🖃 削除 💿 コピー	ᅓ オ-	-バーライト	: 🔹 戻す	✓ 有効化	💿 無効化	移動 - 📔 使用され	れていないル	ールの強調表	眎				

デフォルトで用意されているポリシーである、Interzone-defaultの設定を変更します。

このポリシーは、ゾーン間通信を全て拒否するポリシーで、順番としては最後に評価されますが、ログ出力が無効になっています。

ここまでの設定では、HTTP(TCP/80)とHTTPS(TCP/443)以外の通信は全て Interzone-default にヒットしますが、ログが出力されないと何が拒否されたのかを判断しにくいので、ログ出力が行われるように設定変更します。

(1) a)「Policies」→ b)「セキュリティ」→ c)「interzone-default」が選択された状態にして、d)「オーバーライド」をクリックします。

paloalto		Dashboard ACC		Monitor	Policie	s Obj	ects N	letwork Devi	се				📥 コミット	֊ 🧉 阔 Config	」▼ 및検索
															ら ③ヘルプ
■ セキュリティ b)	٩		_											3個の)項目s 🔁 🗙
A DoS															
💀 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
び 復号 ふ トンネル検査 マブリケーション オーバーライド マブリケーション オーバーション オーバーライド マブリケーション オーバーション オーバーライド マ	1	allow outbound web	none	universal	🊧 Trust	any	any	any	闷 Untrust	any	any	💥 http 🌟 service-https	📀 許可	none	
◎ 認証	1 2	intrazone-default	none	intrazone	any	anv	anv	any	(intrazone)	any	anv	any	😞 क्षेत्र	none	none
Ĵ€DoS プロテクション	3	interzone-default 🧇	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none C)
				d)	٦										
-	Ð	追加 🖃 削除 🚳 コピー	🍬 オ·	ーバーライド	* 戻す	🖌 有効化	圆 無効化	移動 - 📔 使用され	っていないル	ールの強調表	듃				

(2) a)「アクション」で、b)「セッション終了時にログ」にチェックを入れて、c)「OK」をクリックします。

セキュリティ ポリシー	- ルール - predefined			0
全般 アクション a)			口グ設定	
アクション	Deny ICMP 送信到達不能	~	 セッション開始時にログ ゼッション終了時にログ 	
プロファイル設定			ログ転送 None	V
プロファイル タイプ	None	~		
			C) () **	ンセル

(3) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

(DNS が許可されていないので、ここではまだ通信確認は行いません。 コミットも次セクションの DNS 設定が終わってからでも構いません。) 11. App-ID

App-ID は、アプリケーション・シグネチャ、プロトコル・デコーディング、ヒューリスティクスなどの複数の技術を使ってアプリケーションを識別する機能です。

以降、App-ID を使ったポリシーを設定して、その動作を確認します。

11.1.DNS を許可する

前セクションで、全許可ポリシーを削除して、HTTP(TCP/80)とHTTPS(TCP/443)だけを許可する設定に変更したので、 DNS が許可されていません。よって、ポリシーのアプリケーションで DNS を指定して、明示的に許可する設定を行います。 また、本ガイドでは、DNS の Traffic ログは出力しないように設定することにします。

[DNS の Traffic ログ出力を止める理由]

クライアント PC からインターネットへアクセスすると、以下画面のように、DNS ログが多数出力されます。

		Dashboard	ACC	Monitor	Policies	Objects	Network	Device				書コミッ	ト 💣 🖓 Config 🗸 🤇
													F100 🔽 😋 (
▼@□∥	•											and an	⇒ x ⊕ I
く トラフィック		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由
していたいないのです。 していたのでのです。	Þ	02/08 00:08:15	end	Trust	Untrust	192.168.45.32		54.248.231.30	443	ssl	allow	allow outbound	tcp-rst-from-client
NildFireへの送信	D	02/08 00:08:05	end	Trust	Untrust	192.168.45.32		54.248.221.72	443	ssl	allow	allow outbound	tcp-rst-from-client
道データ フィルタリング	Ð	02/08 00:08:05	end	Trust	Untrust	192.168.45.65	•••••	192.168.55.2	53	dns	allow	allow outbound	aged-out
コーザー ID	Ð	02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
🙆 トンネル検査	D	02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
設定 ついて=1	Ð	02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
	D	02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
認証	Ð	02/08 00:08:04	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
「「統合済み	Ð	02/08 00:08:03	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
マロアプリケーション スコープ	Ð	02/08 00:08:03	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
10 サマリー	Đ	02/08 00:08:03	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
№ 変化モニター	Ð	02/08 00:08:02	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
御谷成モニター	D	02/08 00:08:02	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
○ ネットワーク モニター	B	02/08 00:08:02	end	Trust	Untrust	192,168,45,65		192.168.55.2	53	dns	allow	allow outbound	aged-out
トラフィック マップ	P	02/08 00:08:01	end	Trust	Untrust	192.168.45.32		54.248.95.36	443	web-browsing	allow	allow outbound	tcp-fin

本ガイドで行う以降の動作確認時には、DNS 以外の Traffic ログを確認したい場合が多いので、それらのログを見やすく するために、DNS の Traffic ログは出力しないように設定することにします。

11.1.1. 設定

(1) a)「Policies」 \rightarrow b)「セキュリティ」 \rightarrow c)「追加」をクリックします。

paloalto Dashboard ACC Monitor Objects Network Device 📥 コミット 🧬 🖓 Config 🗸 🔍 検索 Policies 😋 💿 ヘルプ ٩. 3個の項目s 🗙 📟 セキュリティ b) ▲ QoS 職ポリシー ベース フォワ 名前 タグ タイプ ゾーン アドレス ユーザー HIP プロファイル ゾーン アドレス アプリケーション サービス アクション プロファイル オプション 🔓 復号 1 allow outbound web none universal M Trust any any any M Untrust any any 👷 http 🕑 許可 none ▲ トンネル検査
 ■ アプリケーション 👷 service-http: 2 intrazone-default 🕸 none intrazone any any any (intrazone) any any 🕑 許可 none 🎭 1311 any ↓ ↓ DoS プロテクション 3 interzone-default 🥎 none interzone any any any any ◎ 拒否 any c) 😫 追加 📑 削除 🔞 コピー 🄏 オーバーライド 🍵 戻す 🖉 有効化 💿 無効化 移動 🛛 📃 使用されていないルールの強闘表示

(2) a)「全般」→ b)名前に「DNS」と入力します。

セキュ	リティポ	リシールーノ	r				0
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	
<u>a)</u>	名前	DNS	b)				
JL	ール タイプ	universal (defau	it)				~
	内容						
	タグ						_
							*
						0K ++>	セル
						DK ++>	t

15

(3) a)「送信元」→ b)「追加」→ c)「Trust」を選択します。

セキュ	リティポリ	リシールーノ	٢						0
全般	送信元	ユーザー	宛先	アプリケーシ	ョン	サービス/URL カテゴ!	ノ アク	ション	
」いす	a) Thờ				🗹 ហទ្	「わか			
🔳 送(言元ゾーン ▲				🔲 送	言元アドレス ▲			
∑ µ	Trust	C)							
b)									-1
🕂 追加	□■削除				+追加	□ ■ 削除			- 1
					Neg	ate			
							OK	キャン	セル

(4) a)「宛先」→ b)「追加」→ c)「Untrust」を選択します。

セキュ	リティポ	ノシー ルーノ	٢					0
全般	送信元	ユーザー	宛先	アプリケーシ	/ヨン	サービス/URL カテゴ!	ノ アクション	
選択		~	a)		🗹 W3	『れか		
一 宛:	先ゾーン 🔺				- 宛:	売アドレス ▲		
	Untrust	C)						
	-							
D) 于追加	□ ■削除				🕂 追加	1 🖃 削除		el.
-					Neg	ate		
						(ОК + +7	セル

(5) a)「アプリケーション」 → b)「追加」で表示されたフォームに c)「dns」と入力して、「dns」を選択します。



(6) 「サービス/URL カテゴリ」のサービスは、「application-default」のまま、URL カテゴリも「いずれか」のままとします。 (application-default の意味については、後述します。)

セキュリティ ポリシー ルール			0
全般 送信元 ユーザー 宛先 アプリケー	ーション	サービス/URL カテゴリ	アクション
application-default	🗹 N3	『れか	
■ サービス ▲	UR	∟ カテゴリ 🔺	
● 追加 ● 削除	+ 追加	□ ■ 削除	_
			OK キャンセル

(7) a)「アクション」 \rightarrow b)アクションは「Allow」のままとし、c)「セッション終了時にログ」のチェックを外します。 d)「OK」をクリックします。

セキュ	リティポリ	ノシー ルーノ	ŀ						0
全般	送信元	ユーザー	宛先	アプリケーシ	′ヨン	サービス	/URL カテゴリ	アクション	
アクシ	ョン設定				ログ語	定		a)	
	アクミ	ンヨン Allow	・送信到達ス	b) 下能		ログ転送	 セッション開始 セッション終了 None 	台時にログ 7時にログ <mark>C)</mark>	V
707	ファイル設定 - プロファイル ク	タイプ None		-	その代 Qa	の設定 スケジュール S マーキング	None		v
							□ サーバー レスフ	ポンス検査の無効化	:
							d)	ОК キャン	セル

(8) 「DNS」ポリシーが選択された状態で、a)「移動」 → b)「上へ」をクリックします。

paloalto	1	Dashboard ACC	;	Monitor	Policie	is Ob	jects	Network Devi	ce				-	y ト 💰 😡 Con	fig・Q.検索
															S ()~JL
💴 セキュリティ	9	-												4 1	1の項目5 🔫
P NAT							設備元			8 1.		1			
ポリシー ベース フォワーディング		名前	97	タイプ	ソーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
登号 登号 ひゃん検査 マブリケーション オーバーライド マグリケーション オーバーライド マブリケーション オーバーライド マ	1	allow outbound web	none	universal	(AN) Trust	апу	any	any	(22) Untrust	any	any	👷 http 🌟 service-https	🖸 許可	none	
2 認証	- 2	DNS	none	universal	PR Trust	any	any	● 最上部へ	Por Untrust	any	drs drs	🙊 application-default	⊘ 許可	none	none
Ĵ∎DoS プロテクション	3	intrazone-default	none	intrazone	апу	апу	алу		(intrazone)	any	апу	any	◎ 許可	none	none
	4	interzone-default 🥎	none	interzone	any	any	any		any	any	any	any	◎ 报香	none	
								● 最下部へ							
		追加 🖃 劇験 🌖 コピ	- 🐐 A	ーパーライト	* ● 脱す		◎ 無効化	移動・日) 使用さ	れていないル	ールの強調	表示				

以下が DNS を上に移動した状態です。

															S 0~
📾 セキュリティ	9													41	の項目1 📑
P NAT							送信元			666					
🔹 ポリシー ベース フォワーディング		名前	47	917	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	PFLX	アプリケーション	サービス	アクション	プロファイル	オプション
◎愛 ボリシー ヘース フォワーティンク 含 登号 品 トンネル検査 篇 アプリケーション オーバーライド 第 20日	1	DNS	none	universal	pog Trust	any	any	any	pre Untrust	any	🛄 dns	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	⊘ 許可	none	none
	2	allow outbound web	none	universal	pag Trust	any	апу	any	pag Untrust	any	any	👷 http. 🌟 service-https	🗢 許可	none	
∎DoS プロテクション	3	Intrazone-default	none	intrazone	апу	апу	апу	any	(intrazone)	any	апу	any	◎ 許可	none	none
	4	interzone-default 🥎	none	interzone	апу	шпу	any	any 💽	any	any	апу	any	◎ 拼音:	none	

(10)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.1.2. Traffic ログのクリア

過去に発生した Traffic ログを消去します(新しく発生する Traffic ログを見やすくするため)。

(1) a)「Device」 \rightarrow b)「ログ設定」で表示された画面を一番下までスクロールし、c)「トラフィックログのクリア」をクリックします。

paloalto	Dashboard ACC	Monitor Policies	Objects Network	Device
				<u>a)</u>
 WM 情報ソース ▶ □ 証明書の管理 ■ 広告ページ 			セキュリティ	違反の期間 ィ ポリシー タグ
□ ログ設定 b) ▼□ サーバー フロファイル	ログの管理			
SNMP トラップ Syslog	トラフィック ログのクリア C) 脅威、URL、およびデータ ログのクリ	7		
🗟 電子メール 🗟 HTTP	設定 ログのクリア			
Retflow	HIP マッチ ログのクリア			
LDAP	アラーム ログのクリア トンネル、GTP ログのクリア			
Kerberos SAML アイデンティティ フ	ユーザー ID ログのクリア			
▲マルチ ファクター認証	認証 ログのクリア			

(2) 「はい」をクリックします。



- 11.1.3. ポリシーの動作確認
- (1) クライアント PC の Web ブラウザからインターネットのいくつかの Web サイトへアクセスします。
- (2) a)「Monitor」 → b)「トラフィック」で、「アプリケーション」が DNS のログが出力されなくなったことを確認します。

		Dashboard	ACC	Monitor	Policies	Objects	Network	Device				含コミッ	ト 省 🖓 Config 🕶 🤇
		· · · · · · · · · · · · · · · · · · ·	4	a)				di.					10 👻 😪
													⇒ × ⊕ I
ペトラフィック b)		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由
log URL フィルタリング	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		52.222.203.12	443	web-browsing	allow	allow outbound	tcp-fin
NildFireへの送信	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.7	443	facebook-base	allow	allow outbound	tcp-fin
■ データ フィルタリング ■ HTD マッチ	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.7	443	facebook-base	allow	allow outbound	tcp-fin
コーザー ID	Ð	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		199.96.57.6	443	twitter-base	allow	allow outbound	tcp-fin
▲ トンネル検査	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		52.222.203.12	443	web-browsing	allow	allow outbound	tcp-fin
 設定 システム 	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.7	443	ssl	allow	allow outbound	tcp-fin
アラーム	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.7	443	ssl	allow	allow outbound	tcp-fin
	Ð	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		104.71.146.45	80	web-browsing	allow	allow outbound	tcp-fin
1回 統合済み	D	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		130.211.31.19	443	web-browsing	allow	allow outbound	tcp-fin
アロアプリケーション スコープ	D	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.7	443	ssl	allow	allow outbound	tcp-fin
🔡 サマリー	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.7	443	ssl	allow	allow outbound	tcp-fin
№ 変化モニター	Þ	02/08 00:23:41	end	Trust	Untrust	192.168.45.32		31.13.82.36	443	facebook-social-	allow	allow outbound	tcp-fin

11.2. [参考] application-default とは

DNS ポリシーのサービスでは、application-default を選択しました。

application-defaultとは、「各アプリケーションに、事前に指定されている(いくつかの)サービス」です。

具体的にどのようなサービスが事前に定義されているのかを確認してみましょう。

(1) a)「Objects」→ b)「アプリケーション」→c)検索フォームに「dns」と入力します。
 表示されたアプリケーションの中から、d)「dns」をクリックします。





(2) dns アプリケーションの詳細が表示されます。

以下の「標準ポート」がサービスに該当します。

アプリケーション				0
名前:	dns			
内容:	The Domain Name System (DNS) stores and associates many types of informati domain names (computer hostnames) to IP addresses, as the ""phone book" fr readable computer hostnames, e.g. www.paloaltonetworks.com, into the IP add for delivering information. It also stores other information such as the list of ma a given domain.	ion with de or the Inte dresses tha ill exchang	omain names, it trai ernet. It translates h at networking equip e servers that accep	nslates iuman- ment needs pt e-mail for
追加情報:	Wikipedia Google Yahoo!			
標準ポート: 依存:	tcp/53, udp/53,5353			
暗黙的に使用:				
特徵	分類			
セキュリティを回避する:	no カテゴリ:	networki	ng	
帯域幅を消費する:	no サプカテゴリ:	infrastru	cture	
悪意のあるソフトウェアに利用され	1 yes テクノロジ:	network-	protocol	
ວ:	עקל:	4	カスタマイズ	
ファイルの転送:	no			
脆弱性が判明している:	yes		カフタマイプ	
他のアプリケーションをすり抜ける せる・		3600	カフタマイプ	
利用さわやすい。		30	177 ST A	
広く使われている。	TCP Half Closed (抄):	120		
12 C DONC C	yes TCP Time Wait (抄):	15	JA7 81 A	
	App-ID 対応:	yes		
- 99				編集
			(別じる

DNS が利用するサービスは、一般的に UDP/53 が多いですが、 プライマリ DNS とセカンダリ DNS の間で使われるゾーン転送は、TCP/53 が使われます。 また、Multicast DNS (RFC6762) は、UDP/5353 が使われます。

このように、DNS だけでも複数のサービスが存在していますが、PA Firewall では、サービスに application-default を指定することで、ポリシー1 行だけで、「TCP/53 or UDP/53 or UDP/5353」 且つ 「DNS プロトコルであること」という条件 (=AND 条件)で許可(または拒否)することができます。

11.3.NTP を許可する

マネージメントインターフェイスを Trust ゾーンに接続したので、マネージメントインターフェイスが外部 NTP サーバーと時 刻同期するには PA Firewall で許可する必要があります。 また、Windows Server も外部 NTP サーバーとの同期を行いたいので、NTP を許可することにします。

(1) a)「Policies」→ b)「セキュリティ」で、c)「DNS」ポリシーが選択された状態で、d)「追加」をクリックします。 (新しく追加されるポリシーは、選択したポリシーの下に追加されるようになっています。)

paloalto	1	Dashboard ACC		Monitor	Policie	es Ob	jects	Network Devi	ce				き コミット	🔒 🔕 Config	Q 検索
														2	・ ②ヘルプ
📾 セキュリティ b)	•													4 個の1	8目s 🕀 🗙
ア NAI ふ QoS 開始ポリシー ベース フォワーディング		名前	91	タイプ	ゾーン	アドレス	送信元	HIP プロファイル		8先 アドレス	アプリケーション	サービス	アクション	プロファイル	オブション
6 復号	1	DNS	none	universal	(20) Trust	any	any	алу	(20) Unbrust	any	🛄 dns	💥 application-default	♥ 許可	none	none C)
 トンネル検査 アプリケーション オーバーライド 認証 	2	allow outbound web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	× http × service-https	💙 許可	none	8
↓ DoS プロテクション	3	intrazone-default 😔	none	intrazone	any	any	any	any	(intrazone)	any	any	any	❷ 許可	none	none
	4	interzone-default 🧐	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	
	••••)	* ×-	-パーライト	: 10 原寸	▽有効化	◎ 無効化	移動 • 🗖 体田式	わていないル		R				

(2)「全般」の名前に「NTP(任意)」と入力します。

セキュ	リティ ポ	リシールー	r				0
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	
	名前	NTP					
Л	ール タイプ	universal (defau	ılt)				-
	内容						
	タグ						-
						OK キャン	セル

(3) 「送信元」は「Trust」を選択します。

セキュリティ ポリシー ルール ()											
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション					
1 1/1	ずれか			🗹 l	いずれか						
■ 送	信元ゾーン ▲			🗖 3	■ 送信元アドレス 🔺						
V (pa) Trust										

(4) 「宛先」は「Untrust」を選択します。

セキュリティ ポリシー ルール										
全般	送信元	ユーザー	宛先	アプリケーシ	(ヨン	サービス/URL カテゴリ	アクション			
選択		-			🗹 W3	『れか				
日 宛:	先ゾーン ▲	_			2 宛:	先アドレス 🔺				
V [22	Untrust									

(5) 「アプリケーション」は「ntp」を選択します。

セキュリティ ポリシー ルール											
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション					
L 113	『れか										
7	プリケーショ	× ▲									
	ntp										

(6) 「サービス/URL カテゴリ」は「application-default」を選択します。

セキュリティ ポリシー ルール ⑦											
全般	送信元	ユーザー	宛先	アプリケーシ	/ヨン	サービス/URL カテゴリ	アクション				
applica	tion-default	-			🗹 613	『れか					
サ・	-ピス ▲				UR	L カテゴリ ▲					

(7) 「アクション」は「allow」であることを確認し、「OK」をクリックします。

セキュ	リティポリ	シールーノ	L						0
全般	送信元	ユーザー	宛先	アプリケー	ション	サービス	/URL カテゴリ	アクション]
アクシ	ョン設定				ログ語	段定			
	アクシ	ョン Allow		~			🗌 セッション開始	自時にログ	
		ICMP) 送信到達	不能	•		☑ セッション終う	了時にログ	
						ログ転送	None		-
					その作	他の設定			
707	アイル設定					スケジュール	None		-
7	プロファイル タ	イプ None		~	Q	oS マーキング	None		-
							- サーバー レスス	ポンス検査の無効化	К
					-				
								OK +73	レセル

(8) 以下のように、「DNS」の下に「NTP」ポリシーが追加されます。

		Dashboard ACC		Monitor	Policie	es Obj	ects N	letwork Devi	се				舎コミット	💣 🛛 👰 Config 🗸	9、検索
														9	る へ ルプ
📟 セキュリティ	٩													5 個の項	[s 🔁 🗙
₩ NAT							送信元		3	8先					
😳 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	🕅 Trust	any	any	any	🛍 Untrust	any	📰 dns	👷 application-default	📀 許可	none	none
トンネル検査 アプリケーション オーバーライド	2	NTP	none	universal	(22) Trust	any	any	any	(1921) Untrust	any	📰 ntp	💥 application-default	🕑 許可	none	
8. 認証	3	allow outbound web	none	universal	🕅 Trust	any	any	any	🕅 Untrust	any	any	🗶 http	📀 許可	none	
↓ DoS プロテクション												🗶 service-https			
	4	intrazone-default 🧇	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
	5	interzone-default 🚳	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	B

- (9) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (10) a)「Monitor」→ b)「トラフィック」で、NTP(UDP/123)が許可されたログが出力されていることを確認してください。 (▲のフォームに c)「port.dst eq 123」と入力して、 をクリックすると、宛先ポート:123 だけに絞込み表示されます。)

patoatto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device		高コミッ	🕨 💣 🎑 Config 🕶	9.検索
											1 v v	③ヘルプ
Valat h	۹ (۱	ort.dst eq 123)	:)								🖶 🗶 🖶	0 🧰 🛛
		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宠先	IP プロトコル	苑先ポート	アプリケーション	アクショ
GURL フィルタリング	Ø	03/11 16:07:18	end	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	ntp	allow
NildFireへの送信	D	03/11 16:06:14	end	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	ntp	allow
↓ デーダ フィルダリング ↓ ↓	ID.	03/11 16:05:07	end	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	ntp	allow
III ユーザー ID	Ð	03/11 16:04:01	end	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	ntp	allow
合トンネル検査	Ø	03/11 16:01:47	end	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	ntp	allow
R定 し システム	P	03/11 16:00:13	drop	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	not-applicable	deny
アラーム	D.	03/11 15:59:09	drop	Trust	Untrust	192.168.45.11	acme\panagent	ntp-b2.nict.go.jp	udp	123	not-applicable	deny

(11) CLI で NTP サーバーへ到達できていることを確認します。 NTP サーバーへ到達できれていれば、reachable が yes になります。

admin@PA-VM> show ntp

NTP state: NTP not synched, using local clock NTP server: ntp.nict.jp status: rejected reachable: yes authentication-type: none

(時刻同期ができると、status: synched となりますが、10分弱かかる場合があります。)

11.4. YouTube を拒否する

このセクションでは、YouTubeを拒否するポリシーを設定します。

例えば、「業務上、YouTubeを使う必要がないので、アクセスさせない」という要件が存在することを想定します。

11.4.1. 設定

(1) a)「Policies」→ b)「セキュリティ」で表示されたポリシーで、「allow outbound web」の上にポリシーを入れたいので、
 c)「NTP」を選択した状態で、d)「追加」をクリックします。

		Dashboard ACC		Monitor	Policie	s Obj	iects N	letwork Devi	ce				📥 コミッ	ト 💣 阔 Config] ▼ Q.検索
															S @~117
■ セキュリティ D)	٩													5 個0	D項目s 🐱
							送信元		8	纬					
🗟 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
◎ 復号	1	DNS	none	universal	699 Trust	anv	anv	any	622 Untrust	anv	= dos	Se application-default	🔊 ¥ 🗃	none	none
(込)トンネル検査 アプリケーション オーバーライド	2	NTP	none	universal	🕅 Trust	any	any	any	🚧 Untrust	any	📰 ntp	💥 application-default	📀 許可	none	🗈 C)
参認証 € DoS プロテクション	3	allow outbound web	none	universal	(120) Trust	any	any	any	🚧 Untrust	any	any	☆ http ☆ service-https	❷ 許可	none	
	4	intrazone-default 🧇	none	intrazone	any	any	апу	any	(intrazone)	any	any	any	🕑 許可	none	none
	5	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	
	d	l)													
	÷	追加 🖃 削除 💿 コピー				✔ 有効化	💿 無効化	移動 - 📄 使用され	れていないル	ールの強調表	示				

(2) a)「全般」→ b)名前に「YouTube(任意)」と入力します。



(3) 「送信元」は「Trust」を選択します。

セキュリティ ポリシー ルール											
アクション											

(4) 「宛先」は「Untrust」を選択します。

セキュ	リティポリ	ノシールーノ	r					0
全般	送信元	ユーザー	宛先	アプリケーシ	ョン	サービス/URL カテゴリ	アクション	
選択		-			🗹 เกร	『れか		
三 宛:	先ゾーン ▲				- 宛	先アドレス ▲		
V [22]	Untrust							
_								

(5) a)「アプリケーション」 \rightarrow b)「追加」で表示されたフォームに「youtube」と入力して、c)「youtube」を選択します。

セキュ	リティポ	リシールーノ	L			0
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション
103	ずれか			a)		
= 7	プリケーショ	× ▲				
	youtube	C)				_
	-					
b)						
⊕ 追加	0 - 削除					
						OK キャンセル

(6) 「サービス/URL カテゴリ」は、「application-default」を選択します。

セキュ	リティポ	リシールーノ	r					0
全般	送信元	ユーザー	宛先	アプリケーシ	ョン	サービス/URL カテゴリ	アクション	
applica	tion-default	-			🗹 W	ずれか		
サ・	ーピス 🔺					೩ カテゴリ ▲		

(7) a)「アクション」 \rightarrow b)「Deny」を選択し、c)「OK」をクリックします。

セキュリティ ポリシー ルール				0
全般 送信元 ユーザー 宛先 アプリケーシ	'ヨン サービス	/URL カテゴリ	アクション	
アクション設定	ログ設定		a)	
アクション Deny D)		セッション開始	台時にログ	
ICMP 送信到速不能		✓ セッション終了	了時にログ	_
	ログ転送	None		~
	その他の設定			
	スケジュール	None		~
フロファイル ダイフ None	QoS マーキング	None		~
		□ サーバー レスフ	ポンス検査の無効化	
		c)	OK キャン	セル

(8) 以下のように、「allow outbound web」の上に「YouTube」を拒否するポリシーが追加されます。

paloalto	1	Dashboard ACC		Monitor	Policie	s Ob	jects	Network Devi	Ce				含コミッ	ト 💣 🔯 Config	g - Q.検 索
															S @~~
💴 セキュリティ	٩													8個(の項目s 🔿 🗙
PNAT							送信元			19 5					
■ ポリシー ベース フォワーディング [●] 復号		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	апу	any	🕅 Untrust	any	📰 dns	👷 application-default	📀 許可	none	none
(M) トンネル検証 目 アプリケーション オーパーライド	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🛄 ntp	👷 application-default	📀 許可	none	
8 RE	3	Youtube	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔝 youtube	👷 application-default	◎ 拒否	none	
(Ĵ DoS プロテクション	4	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	апу	💥 http 🎉 service-https	🕑 許可	none	
	5	intrazone-default 🥹	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
	6	interzone-default 🧐	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(9) ブロックした時に、応答ページが出るようにします。

a)「Device」 → b)「応答ページ」 →「アプリケーション ブロック ページ」の右横の c)「無効」をクリックします。

paloalto	Dashboard ACC Monitor Policies	Objects Network Device a)	총 그
 ID VM 情報ソース 	९ १८७७	アクション	場所
▶ 局証明書の管理 ◎ 応答ページ b)	アンチウイルス/アンチスパイウェア ブロック ページ アブリケーション ブロック ページ	(một)	デフォルト
▲ ロク設定 ▼	キャプティブ ポータル認証ページ データ フィルタリング ブロック ページ		デフォルト
ロ Sivier トラック III Syslog 副 電子メール	ファイル ブロッキング統行ページ ファイル ブロッキング ブロック ページ		デフォルト
🗟 НТТР	GlobalProtect アプリケーションのヘルプ ページ		デフォルト

(10) a)「有効化 アプリケーション ブロック ページ」にチェックを入れ、b)「OK」をクリックします。



(11)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.4.2. 通信確認

- (1) クライアント PC から、YouTube (<u>www.youtube.com</u>) ヘアクセスします。
- (2) ブロックページが表示されます。

Application Blocked Access to the application you were trying to use has been blocked in accordance with company policy. Please contact yo system administrator if you believe this is in error. User: 192.168.45.32	≊ ☆
Access to the application you were trying to use has been blocked in accordance with company policy. Please contact ye system administrator if you believe this is in error. User: 192.168.45.32	
User: 192.168.45.32	<i>'</i> our
Application: youtube-base	

11.5. YouTube のストリーミングのみ許可する

今度は、「YouTube ストリーミングの視聴は許可するが、それ以外(動画アップロード等)の行為は拒否する」という要件を 想定した設定を行います。

11.5.1. 設定

(1) a)「Policies」 \rightarrow b)「セキュリティ」で表示されたポリシーで、「Youtube」の上にポリシーを入れたいので、c)「NTP」を 選択した状態で、d)「追加」をクリックします。

															S @~117
📟 セキュリティ b)	•													6 個0	の項目s 🗙
A DOS							送信元		3	8先					
💀 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
◎ 復号	1	DNS	none	universal	(22) Trust	any	any	any	(2) Untrust	any	📰 dns	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	📀 許可	none	none
(論 トンネル検査 アプリケーション オーバーライド	2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	🛄 ntp	💥 application-default	📀 許可	none	C C
😓 認証	3	Youtube	none	universal	🕅 Trust	any	any	any	🕅 Untrust	any	jj youtube	% application-default	◎ 拒否	none	
(手DoS プロテクション	4	allow outbound web	none	universal	🕅 Trust	any	any	any	M Untrust	any	any	🙊 http	📀 許可	none	
												× service-https			
	5	intrazone-default 🧇	none	intrazone	any	any	апу	any	(intrazone)	any	any	any	🕑 許可	none	none
	6	interzone-default 🥎	none	interzone	any	any	апу	any	any	any	any	any	◎ 拒否	none	
	d +)	* * -	-パーライド	* Ē4	☑ 有効化	◎ 無効化	移動,一面 体田之	やていたいり	一川の冷調す	-				

(2) a)「全般」→ b)名前に「Youtube-streaming(任意)」と入力します。

セキュ	リティポ	リシールーノ	r				0
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	
a)	名前	Youtube-stream	ing 🛔)			
μ	ール タイプ	universal (defau	lt)				-
	内容						
	タグ						
							-
						OK キャン	セル

(3) 「送信元」は「Trust」を選択します。



(4) 「宛先」は「Untrust」を選択します。

セキュリティ ポリシー ルール											
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション					
選択		~		ジ い	ずれか						
一宛	先ゾーン 🔺			3	!先アドレス ▲						
V (20)	Untrust										

- (5) a)「アプリケーション」→ b)「追加」で表示されたフォームに「youtube-steaming」と入力して表示された、
 c)「youtube-streaming」を選択します。
 さらにもう一度、b)「追加」で表示されたフォームに「youtube-base」と入力して表示された、d)「youtube-base」を選択します。
 - ※ ここで2つのアプリケーションを選択した理由は、アプリケーションによっては「依存関係」が存在するためです。 アプリケーションの依存関係については後述します。

セキュリティ ポリシー ルール			0
全般 送信元 ユーザー 宛先	アプリケーション	サービス/URL カテゴリ	アクション
🔲 いずれか	a)		
■ アプリケーション ▲			
voutube-base			
u)			
b) ● 追加 ■ 削除			_
		_	
			OK キャンセル

(6) 「サービス/URL カテゴリ」は、「application-default」を選択します。

セキュリティポリシールール (
全般 送	信元	ユーザー	宛先	アプリケーシ	/ヨン	サービス/URL カテゴリ	アクション					
application-d	default	~			🗹 ເບອ້ານກ							
🔲 サービス	۸ 🛋				🔲 URL カテゴリ 🔺							

(7) a)「アクション」 \rightarrow b)「Allow」を確認し、c)「OK」をクリックします。



(8) 以下のように、「Youtube」を拒否するポリシーの上に「Youtube-streaming」を許可するポリシーが追加されます。

paloalto	1	Dashboard ACC		Monitor	Policie	s Ob	jects	Network Dev	ce				📥 コミット	💣 Config	 Q.検索
														5	3 (D~117
📟 セキュリティ	٩													7個の	項目s 🗙
PAT							送信元		5	图先					
ポリシー ベース フォワーディン	17	名前	911	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
□ 復号	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔟 dns	💥 application-default	🕑 許可	none	none
() トンネル検査	5 2	NTP	none	universal	(22) Trust	any	any	any	(20) Untrust	any	m ntp	👷 application-default	📀 許可	none	
 急認証 しのS プロテクション 	3	Youtube-streaming	none	universal	(200) Trust	any	any	any	(120) Untrust	any	youtube-base	X application-default	🙁 許可	none	
Contraction in the second second	4	Youtube	none	universal	(22) Trust	any	any	any	(22) Untrust	any	j youtube	🔆 application-default	◎ 拒否	none	
	5	allow outbound web	none	universal	(77) Trust	any	any	any	(20) Untrust	any	any	🗶 http 🎉 service-https	🕑 許可	none	
	6	intrazone-default 🔇	none	intrazone	any	any	any	any	(intrazone)	апу	any	any	⊘ 許可	none	none
	7	interzone-default 🍪	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(9) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.5.2. 通信確認

- (1) クライアント PC から YouTube (www.youtube.com) ヘアクセスし、動画を見ることができることを確認します。
- (2) 適当な動画ファイルを使って、YouTube への Upload を試みます。

Web ブラウザ内の右上にある a) 🏧 アイコンをクリックし、b)「動画をアップロード」を選択し、表示された画面にファイルを ドラッグ & ドロップします。



(3) 以下のように、エラーになります。

	ロ ア	ップロ	I−۴ - YouTube ×				86
*	\rightarrow	G	● 保護された通信	https://www.youtube.com/upload			
	=	Þ	YouTube ^{JP}	検 索 Q		<u>±</u>	Û
				ネットワーク上でデータを送信中にエラーが発生しました。ネットワーク接続を確認してから、もうー) ドしてみてください。	度アップロー	×	
					動画の管理	+ 他の動画を追加	٥

(4) a)「Monitor」→ b)「トラフィック」で表示されたログのアプリケーションで、c)「youtube-uploading」を見つけます。 そのログのアクション列を見ると、拒否(reset-both)されていることが分かります。

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device				3	当コミット 🗗 😡	Config - Q 検索
				a)									手動	💌 😋 💿 ヘルプ
▼ [™] ⊓#														x 🕀 📪 🛱 🖸
端、トラフィック D		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IP プロトコル	アプリケーション	アクション	ルール	セッション終了理由
GURL フィルタリング	Þ	02/08 01:21:21	end	Trust	Untrust	192.168.45.32		172.217.31.142	443	tcp	google-base	allow	allow outbound web	tcp-fin
NildFireへの送信	Þ	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.31.134	443	tcp	google-base	allow	allow outbound web	tcp-fin
·····································	P	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.31.141	443	tcp	google-base	allow	allow outbound web	tcp-fin
IN ユーザー ID	P	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.26.14	443	tcp	youtube-base	allow	Youtube-streaming	tcp-fin
トンネル検査	P	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.26.14	443	tcp	youtube-base	allow	Youtube-streaming	tcp-fin
し 設定	P	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.31.142	443	tcp	ssl	allow	allow outbound web	tcp-fin
アラーム	P	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.26.14	443	tcp	youtube-base	allow	Youtube-streaming	tcp-fin
認証	D	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.26.14	443	tcp	youtube-base	allow	Youtube-streaming	tcp-fin
● ポ合済み	P	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.26.14	443	tcp	youtube-base	allow	Youtube-streaming	tcp-fin
マロアプリケーション スコープ	D	02/08 01:20:31	end	Trust	Untrust	192.168.45.32		172.217.31.131	443	tcp	web-browsing	allow	allow outbound web	tcp-fin
🔡 サマリー	P	02/08 01:20:31	end	Trust	Untrust	192.168.45.32		172.217.31.142	443	tcp	google-base	allow	allow outbound web	tcp-fin
◎ 変化モニター	Ð	02/08 01:20:31	end	Trust	Untrust	192.168.45.32		172.217.31.131	443	tcp	google-base	allow	allow outbound web	tcp-fin
() 脅威マップ	D	02/08 01:20:31	end	Trust	Untrust	192.168.45.32		172.217.31.134	443	tcp	google-base	allow	allow outbound web	tcp-fin
🞯 ネットワーク モニター	D	02/08 01:20:29	end	Trust	Untrust	192.168.45.32		172.217.26.14	443	tcp	youtube-base	allow	Youtube-streaming	tcp-fin
トラフィック マップ	ø	02/08 01:20:16	deny	Trust	Untrust	192.168.45.32		172.217.31.143	443	tcp	youtube-uploading	reset-both	Youtube	policy-deny C)
G πyトネット	LO I	02/08 01:20:14	drop	Trust	Untrust	192.168.45.32	•••••	172.217.31.134	443	udp	not-applicable	deny	interzone-default	policy-deny
▼ PDF レポート	D	02/08 01:20:12	drop	Trust	Untrust	192.168.45.32		172.217.31.134	443	udp	not-applicable	deny	interzone-default	policy-deny

(5) [参考] QUIC プロトコル

Chrome で Youtube にアクセスすると、Deny されているのは youtube-uploading だけでなく、UDP/443 も Deny されているログが多数確認されます。

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device					\$_1<	ット 💣 🎯 Config 🗸	Q.検索
0.00000000														手動 👻 😪	のヘルプ
▼ □ = 1	🔍 (a	iction eq deny)												- x -	6 阔
ペートラフィック の 必可		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IPプロトコル	アプリケーション	アクション	ルール	セッション終了理由	KTH
BURL フィルタリング	P	02/04 22:44:05	drop	Trust	Untrust	192.168.45.32		172.217.31.132	443	udp	not-applicable	deny	interzone-default	policy-deny	110
	P	02/04 22:44:03	drop	Trust	Untrust	192.168.45.32		172.217.31.132	443	udp	not-applicable	deny	interzone-default	policy-deny	1.4k
データ フィルタリング	Þ	02/04 22:44:02	drop	Trust	Untrust	192.168.45.32		172.217.31.132	443	udp	not-applicable	deny	interzone-default	policy-deny	1.4k
コーザー ID	P	02/04 22:44:02	drop	Trust	Untrust	192.168.45.32		74.125.155.235	443	udp	not-applicable	deny	interzone-default	policy-deny	110
🔒 トンネル検査	D	02/04 22:44:01	drop	Trust	Untrust	192.168.45.32		172.217.31.132	443	udp	not-applicable	deny	interzone-default	policy-deny	1.4k
- 設定 - システム	P	02/04 22:44:01	drop	Trust	Untrust	192.168.45.32		172.217.31.132	443	udp	not-applicable	deny	interzone-default	policy-deny	1,4k

これは、Chrome ブラウザが Google 関連のサイトにアクセスする際、最初は QUIC プロトコル (Google 独自プロトコル: UDP/443 を利用) を使おうとするからです。

Chrome ブラウザは、QUIC のネゴシエーションができないことが分かると、次に TCP/443 を使うので、PA Firewall で QUIC が許可されていなくても TCP/443 で YouTube 動画を見ることができます。

現在、PA Firewall では QUIC の復号化はサポートしていないので、UDP/443 の暗号化通信を悪用した攻撃の検知が難 しいため、セキュリティの観点から拒否しておくことを推奨しています。

https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Block-QUIC-Protocol/ta-p/120207

11.6. [参考] アプリケーションの依存関係

アプリケーションによっては、依存関係を持つものが存在しています。

依存関係とは、あるアプリケーションを許可したいとき、依存関係のあるアプリケーションも同時に許可しなければ、そのア プリケーションが利用できない、という関係にあります。

具体的に確認してみましょう。

 (1) a)「Objects」→ b)「アプリケーション」→c)のフォームに「youtube-streaming」と入力し、Enter キーを押します。 表示されたアプリケーションで d)「youtube-streaming」をクリックします。

paloalto	Dashboard ACC	Monitor Policies Objects	Networ	k Device			 ふコミット 💰 🎯 Config • 9.検索 ③ へルプ
5 7FL2	Not youtube-streaming	TAN DX C	¥ 🗶	フィルタのクリア			3 一致するアプリケーション
🧐 アドレス グループ	カテゴリ	サブカテゴリ →		テクノロジェ		リスクー	特徵 •
 アブリケーション アブリケーションフィルタ サービス グループ タグ ClobalProtect ドルフズジェクト 	1 general-internet 2 media	1 internet-utility 2 photo-video		3 browser-based		1 20 1 23 1 23	1 セギュリティを応激する 2 帯域機を消費する 2 広く使われている 1 悪意のあるソフトウェアに利用される 3 動弱性 1 転送ファイル
➡ HIP プロファイル	名前	タグ付けされました	カテゴリ	サブカテゴリ	リスク	テクノロジ	農業技工で
マ 🐻 カスタム オブジェクト	google-play		general-intern	et internet-utility	E	browser-based	tcp/443,80,5228,udp/5228
 データ パターン スパイウェア 第2時 	 ■ khan-academy ■ youtube (7 中 1 を表示) 		media	photo-video	8	browser-based	tcp/80,443,udp/443
● #83911 ● URL カテゴリ ▼ ③ セキュリティ プロファイル	would be streaming	d)	media	photo-video	•	browser-based	tcp/80,443

(2) youtube-streaming アプリケーションの詳細が確認できます。

以下の「依存:」と書かれた部分に、「youtube-base」とあります。

よって、「youtube-streaming」を許可する際には、同時に「youtube-base」も許可する必要がある、ということが分かります。

アプリケーション	0
名前: youtube-streaming 標準ボート: tcp/80,443 依存: youtube-base 暗黙的に使用: アクションの拒否: drop-reset 追加情報: Wikipedia Google Yahool	内容: YouTube is a popular free video sharing website which lets users upload, view, and share video clips. Videos can be rated, and the average rating and the number of times a video has been watched are both published. Youtube-streaming identifies video streaming activity on Youtube.
特徴 セキュリティを回避する: yes 他のアプリケーションをすり抜けさ no 帯域幅を消費する: yes 乱用されやすい: no 高のあるソフトウェアに利用され yes る: 広く使われている: yes 別時時性が判明している: yes	オプション TCP タイムアウト (秒): 3600 カスタマイズ TCP Half Closed (秒): 120 カスタマイズ TCP Time Wait (秒): 15 カスタマイズ App-ID 対応: yes
分類 カテゴリ: media サブカテゴリ: photo-video テクノロジ: browser-based リスク: 【 カスタマイズ	編集

(3)「Youtube」ポリシーで、Youtube アプリケーション全てを拒否にしているので、その中に「youtube-base」アプリケーションも含まれています。

よって、Youtube ストリーミングを許可するためには、その「Youtube」ポリシー行の上に、「youtube-base」と 「youtube-streaming」の2つのアプリケーションを許可する必要があります。

						送信元						
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	DNS	none	universal	(20) Trust	any	any	any	(200) Untrust	any	📰 dns	🗶 application-default	📀 許可
2	NTP	none	universal	🛱 Trust	any	any	any	🕅 Untrust	any	📰 ntp	👷 application-default	📀 許可
3	Youtube-streaming	none	universal	🕅 Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	🔮 許可
4	Youtube	none	universal	più Trust	any	any	any	(22) Untrust	any	📰 youtube	🗶 application-default	◎ 拒否
5	allow outbound web	none	universal	(200) Trust	any	any	any	🕅 Untrust	any	any	http service-https	🕑 許可

(4) 更に言えば、「youtube-base」は、「google-base」との依存関係があります。

アプリケーション	0
名前: youtube-base	内容:
標準ポート: tcp/80,443	YouTube is a popular free video sharing website which lets users upload, view, and share video clips. Videos can be rated, and the
依存: google-base	average rating and the number of times a video has been watched are
暗黙的に使用:	photo-upload function to work properly on youtube, customers will
追加情報: Wikipedia Google Yahoo!	have to allow google-docs-base App-ID as well.

(5) 「google-base」は「allow outbound web」の「any」に含まれています。

よって、「youtube-base」を許可するために「google-base」を明示的に許可しなくても、すでに許可されている状態にある、ということです。

				送信元								
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	DNS	none	universal	(20) Trust	any	any	any	(202) Untrust	any	📰 dns	🗶 application-default	📀 許可
2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	📰 ntp	💥 application-default	📀 許可
3	Youtube-streaming	none	universal	🕅 Trust	any	any	any	🕅 Untrust	any	youtube-base	× application-default	📀 許可
4	Youtube	none	universal	ping Trust	any	any	any	🕅 Untrust	any	📰 youtube	👷 application-default	◎ 拒否
5	allow outbound web	none	universal	(200) Trust	any	any	any	M Untrust	any	any	 http service-https 	🕏 許可
			[any][こ、「goo	gle-bas	e」アブリケー	ーションが含まれて	こいる。 ~				

11.7.リスク5の File Sharing をまとめて拒否する

アプリケーションにはそれぞれパロアルトネットワークス社が定めた5段階のリスク値が設定されていて、5がもっともリスクが高いアプリケーションである、という位置付けになっています。

ここでは、「情報漏洩の対策として、リスク5のファイル共有アプリケーションは使わせない」という要件を想定し、その設定 を行います。

11.7.1. 設定前の通信確認

ポリシーで拒否する前に、リスク5のファイル共有アプリケーションへアクセスが可能であることを確認します。 サンプルとして、以下の2つにアクセスします。

(1) クライアント PC から、Google ドライブ (https://drive.google.com) ヘアクセスできることを確認します。

A My Drive - Google Drive X												
← → C ● 保護された通信 https://drive.google.com/drive/my-drive												
Google Drive	Q Search Drive	•										
NEW	My Drive 👻											
My Drive	Quick Access											

(2) クライアント PC から、Transfer Big Files (https://www.transferbigfiles.com) ヘアクセスできることを確認します。

🧭 Transfer	Big Files Free - E ×	8
$\leftrightarrow \ \ni \ G$	▲ 保護された通信 https://www.transferbigfiles.com	
	Transfer, pic Files The easiest way to send large files fastand it's Free! Create an Account Login Or check out the features tour.	

11.7.2. 設定

(1) a)「Objects」 \rightarrow b)「アプリケーション フィルタ」 \rightarrow c)「追加」 をクリックします。

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device			📥 コミット
57817						a)					
マドレス グループ マドレス グループ 地域 コブリケーション/		名前	場所		カテゴリ		Ψ	ブカテゴリ	テクノロジ	リスク	特徴
■ アブリケーション グループ ■ アプリケーション グループ ■ アプリケーション フィルタ b)										
★ サービス 除サービス グループ ◎ タグ		2)									
V 😢 GlobalProtect	.	追加日前除(<u>)</u> コピー								

(2) a)リスクの下の「5」をクリックし、b)サブカテゴリの下の「file-sharing」をクリックすることで、この2つの属性を持つアプ リケーションに絞込み(フィルタ)されます。

(絞込み表示された中に「google-drive-web」および「transferbigfiles」が存在していることを確認してください。)

アプリケーション フィルタ 0 名前 Risk5_file-sharing 🔀 フィルタのクリア 65 一致するアプリケーション cカテゴリ 🔺 リスク 🔺 ブカテゴリ 🔺 テクノロジ 🔺 特徴 ▲ 7 SaaS 65 general-internet 1 audio-streaming 18 browser-bas 65 5 62 セキュリティを回避する 3 email 6 client-server a) 51 乱用されやすい 41 peer-to-peer 8 他のアプリケーションをすり抜けさせる 65 file-sharing b) 59 帯域幅を消費する 55 広く使われている 65 悪意のあるソフトウェアに利用される 4 internet-utility 4 office-programs 62 脆弱性 10 photo-video 65 転送ファイル 25 proxy 名前 タグ付けされまし カテゴリ サブカテゴリ リスク テクノロジ 標準ポート 5 💷 gnutella general-internet file-sharing peer-to-peer dynamic.tcp.udp III goboogy general-internet file-sharing 5 peer-to-peer 5325,tcp,udp Ⅲ google-drive-web Ⅲ google-talk (3 中 1 を表示) 5 general-internet 443,80,tcp file-sharing browser-based 5 dynamic,tcp,udp gtalk-file-transfer general-internet file-sharing peer-to-peer general-internet file-sharing 5 browser-based 80.tcp 💷 hotfile ページ 1/2 ▷ ▷> キャンセル OK

c)名前に「Risk5_file-sharing(任意)」と入力し、d)「OK」をクリックします。

(3) a)「Policies」→ b)「セキュリティ」で表示されたポリシーで、「allow outbound web」の上にポリシーを入れたいので、 c)「Youtube」を選択した状態で、d)「追加」をクリックします。

paloalto	1	Dashboard ACC		Monitor	Policie	s Ob	jects I	Network Devi	ce				🍰 コミツ	ト 💰 🗋 Confi	g ▼ Q 検 索
															🕿 💿 ヘルプ
📾 セキュリティ b)	٩,													7個	の項目s ラ 🗙
2 NAI							送信元			动先					
ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
 ⑦ 復号 ▲ トンネル検査 国 アプリケーション オーバーライド ② 認証 ③ 取正 ③ DoS プロテクション 	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🖽 dns	👷 application-default	🕑 許可	none	none
	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	III ntp	👷 application-default	🕑 許可	none	
	3	Youtube-streaming	none	universal	(122) Trust	any	any	any	យៀ Untrust	any	youtube-base	🗶 application-default	🕑 許可	none	
	4	Youtube	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🛄 youtube	👷 application-default	◎ 拒否	none	🗈 C)
	5	allow outbound web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	🗶 http 🎉 service-https	🕑 許可	none	
	6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
	7	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	
	•	<mark>d)</mark> 追加 日前除 😒 コピー	- 🌣 オ-	-バーライト	: * 頁す	☑ 有効化	◎ 無効化	移動 - 📕 使用さ	れていないル	ールの強調者	友示				

(4) a)「全般」→ b)名前に「Risk5_file-sharing(任意)」と入力します。

セキュ	リティポ	リシールーノ	r				0
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	
<u>a)</u>	名前	Risk5_file-sharir	ng)			
μ	ール タイプ	universal (defau	ilt)				-
	内容						

(5) 「送信元」は「Trust」を選択します。

セキュリティ ポリシー ルール											
全般	送信元	ユーザー	宛先	アプリケーション	/	サービス/URL カテゴリ	アクション				
L 613	ずれか				いず	わか					
■ 送	信元ゾーン 🔺				送信	『元アドレス ▲					
V [0	Trust										

(6) 「宛先」は「Untrust」を選択します。

セキュ	リティポ!	ノシールー	IL					0
全般	送信元	ユーザー	宛先	アプリケーシ	/ヨン	サービス/URL カテゴリ	アクション	
選択		~			🗹 W3	『れか		
三 宛;	先ゾーン ▲				🔲 宛:	先アドレス 🔺		
V (m)	Untrust							

(7) a)「アプリケーション」→ b)「追加」で表示されたフォームに c)「Risk5」の文字列を入れて、作成したアプリケーション フィルタを検索します。 表示された d)「Risk5_file-sharing」を選択します。

セキュリティ ポリシー ルール											
全般 送信元 ユーザー 宛先	アプリケーション	サービス/URL カテゴリ	アクション								
🔲 いずれか	a)										
■ アプリケーション 🔺											
Risk5 C			~								
Risk5_file-sharing d)											
新規 瞬 アプリケーション フィルタ 💼	アプリケーション グループ										
b)											
● 追加 ● 削除											
			OK キャンセル								

(8) 「サービス/URL カテゴリ」は、「application-default」を選択します。

セキュリティ ポリシー ルール (
全般	送信元	ユーザー	宛先	アプリケーシ	′ョン	サービス/URL カテゴリ	アクション				
applicat	ion-default	~	ずれか								
🔳 サ-	-ピス 🔺					೩ カテゴリ ▲					

(9) a)「アクション」 \rightarrow b)「Deny」を選択し、c)「OK」をクリックします。



(10) 以下のように、「allow outbound web」ポリシーの上に「Risk5_file-sharing」を拒否するポリシーが追加されます。

NETWORKS		Dashboard ACC		Monitor	Policie	s Ob	jects	Network Dev	ice				コミッ	r 😅 🖓 Confi	」▼Ч夜郛
															S ()~117
セキュリティ	٩													7個	の項目s ラ 🗙
NAT							送信元		5	珗					
● ポリシー ベース フォワーディング 雪 復号 ▲ トンネル検査 国 マブリケーション オーバーライド		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(20) Trust	any	any	any	(22) Untrust	апу	🛄 dns	👷 application-default	📀 許可	none	none
	2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	mtp	👷 application-default	🔮 許可	none	
プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	🕑 許可	none	
	4	Youtube	none	universal	(20) Trust	any	any	any	pag Untrust	any	youtube	👷 application-default	◎ 拒否	none	
	5	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	🙀 Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	6	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	🔆 http 🎗 service-https	😕 許可	none	
	7	intrazone-default 🛛 🎯	none	intrazone	any	any	any	any	(intrazone)	any	any	any	◎ 許可	none	none
	8	interzone-default 🌍	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(11)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.7.3. 通信確認

(1) クライアント PC から、Google ドライブ (https://drive.google.com) ヘアクセスすると、拒否されることを確認します。



(2) クライアント PC から、Transfer Big Files (https://www.transferbigfiles.com) ヘアクセスすると、拒否されることを確認します。

💋 🍻 Appli	ication Blocked ×	a) [23
$\epsilon \rightarrow \epsilon$	C ● 保護された通信 https://www.transferbigfiles.com	G	☆	:
				1
A	pplication Blocked			
A S)	ccess to the application you were trying to use has been blocked in accordance with company policy. Please contact y stem administrator if you believe this is in error.	our		
U	ser: 192.168.45.32			
A	pplication: transferbigfiles			

(3) a)「Monitor」→ b)「トラフィック」で、ログを確認します。

アプリケーションの「transferbigfiles」と「google-drive-web」が、ルールの「Risk5_file-sharing」で拒否されていること が分かります。

■のフォームに c)「(rule eq Risk5_file-sharing)」と入力し、 🖻 をクリックすると、そのルールにヒットしたログだけに 絞込み表示されます。

または、「ルール」列で「Risk5_file-sharing」を見つけて、それをクリックするだけで、 自動的に**国のフォーム**に c)「(rule eq Risk5_file-sharing)」の文字列が入ります。

JIP paloalto	[Dashboard	ACC	Monitor	Policies	Objects	Network	Device					含コミッ	r 占 🥵 Config 🗸	Q.検索
														F 🛍 💌 😋	③ヘルプ
	Q (n	ule eq Risk5_file-sha	ring) C											⇒ × ⊕	🖻 🛱 🖸
		受信日時	917	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	IP プロトコル	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由	1841
lo URL フィルタリング	P	03/12 11:56:53	deny	Trust	Untrust	192.168.45.32		tbfweb1.transferbigfiles.com	tcp	443	transferbigfiles	reset-both	Risk5_file-sharing	policy-deny	6.3k
NildFireへの送信	P	03/12 11:56:52	deny	Trust	Untrust	192.168.45.32		tbfweb1.transferbigfiles.com	tcp	443	transferbigfiles	reset-both	Risk5_file-sharing	policy-deny	6.4k
■ データ フィルタリング ■ HIP マッチ	P	03/12 11:56:47	deny	Trust	Untrust	192.168.45.32		hkg12s01-in-f110.1e100.net	tcp	443	google-drive-web	reset-both	Risk5_file-sharing	policy-deny	6.5k
コーザー ID	P	03/12 11:56:46	deny	Trust	Untrust	192.168.45.32		hkg12s01-in-f110.1e100.net	tcp	443	google-drive-web	reset-both	Risk5_file-sharing	policy-deny	6,6k

「リスク5のファイル共有アプリケーションのうち、googleドライブだけは業務上必要なので、許可したい」という要件を想定します。

11.8.1. 設定

(1) a)「Policies」→ b)「セキュリティ」で表示されたポリシーで、「Risk5_file-sharing」の上にポリシーを入れたいので、 c)「Youtube」を選択した状態で、d)「追加」をクリックします。

															S @~//
∎tataljtr b)	٩												8 個の項目s 🗙		
☆ ron ▲ QoS ● ポリシーベースフォワーディング ● 投号 ▲ トンネル検査 ■ アプリケーション オーパーライド ● 原語 ■ DoS プロデクション							送信元		,	8先		ーション サービス			
		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション		アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	🔝 dns	👷 application-default	許可	none	none
	2	NTP	none	universal	(20) Trust	any	any	any	🕅 Untrust	апу	m ntp	👷 application-default	📀 許可	none	
	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	🕑 許可	none	
	4	Youtube	none	universal	(20) Trust	any	any	any	(22) Unbrust	any	youtube	💥 application-default	◎ 拒否	none	
	5	Risk5_file-sharing	none	universal	(20) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	× application-default	◎ 拒否	none	
	6	allow outbound web	none	universal	(22) Trust	any	any	any	(201) Untrust	any	any	🔆 http 🗶 service-https	🕑 許可	none	
	7	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	апу	any	◎ 許可	none	none
	8	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(2) a)「全般」→ b)名前に「google-drive-web(任意)」と入力します。

セキュ	2キュリティ ポリシー ルール											
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション						
a)	名前 google-drive-web b)											
μ	ール タイプ	universal (defau	lt)				-					
	内容											

(3) 「送信元」は「Trust」を選択します。



(4) 「宛先」は「Untrust」を選択します。

セキュ	リティポリ	ノシー ルー.	r							
全般	送信元	ユーザー	宛先	アプリケーシ	/ヨン	サービス/URL カテゴリ	アクション			
選択		~			🗹 W3	『れか				
- 宛:	先ゾーン 🔺				🔳 宛:	先アドレス ▲				
V [22]	Untrust									

(5) 「アプリケーション」は「google-drive-web」を選択します。

セキュ	セキュリティ ポリシー ルール ⑦											
全般	送信元	ユーザー	宛先	アプリケーション	サービス/URL カテゴリ	アクション	_					
L 113	「れか											
7	プリケーショ	ン 🔺										
☑ 🗖	google-drive	e-web										

(6) 「サービス/URL カテゴリ」は「application-default」を選択します。

ション	サービス/URL カテゴリ	アクション				
🗹 ເນອກກ						
	∟ カテゴリ 🔺		- 1			
	ション ダ い3	ション サービス/URLカテゴリ ▼ いずれか ■ URLカテゴリ ▲	ション サービス/URLカテゴリ アクション びいずれか ■ URLカテゴリ▲			

(7) a)「アクション」 \rightarrow b)「Allow」を確認し、c)「OK」をクリックします。

セキュリティ ポリシー ルール				0
全般 送信元 ユーザー 宛先 アプリケーシ	ョン サービス	/URL カテゴリ	アクション	
アクション設定	ログ設定		a)	
アクション Allow b)		🗌 セッション開始	台時にログ	
ICMP 送信到递不能		🗹 セッション終了	了時にログ	
	ログ転送	None		•
	その他の設定			
プロファイル設定	スケジュール	None		-
プロファイルタイプ None 💌	QoS マーキング	None		-
		🗌 サーバー レスオ	ポンス検査の無効化	
		c)	OK キャン・	en.
				_

(8) 以下のように、「Risk5_file-sharing」ポリシーの上に「google-drive-web」を許可するポリシーが追加されます。

NETWORKS'		Dashboard ACC		Monitor	Policie	s Ob	jects	Network Dev	се				🏝 コミッ	ト 💰 闷 Confi	g▼♀検索
															🛭 💿 ヘルプ
📟 セキュリティ	۹.													8 個	の項目s 🌛 🗙
NAT QoS ポリシー ベース フォワーディング 復号							送信元			8 %				-	
、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、		名前	97	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
復号 トンネル検査 アプリケーション オーパーライド 認証 DoS プロテクション	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🛄 dns	💥 application-default	资許可	none	none
	2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	m ntp	👷 application-default	📀 許可	none	
	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	2 application-default	🕑 許可	none	
	4	Youtube	none	universal	(22) Trust	any	any	any	(22) Untrust	any	youtube	👷 application-default	◎ 非否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	google-drive-web	💥 application-default	📀 許可	none	B
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	апу	põõ Untrust	any	Risk5_file-sharing	🗶 application-default	◎ 拒否	none	
7	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	% http % service-https	🕑 許可	none	
	8	intrazone-default 🔮	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🖸 許可	none	none
	9	interzone-default	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	B

(9) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.8.2. 通信確認

(1) クライアント PC から、Google ドライブ (https://drive.google.com) ヘアクセスできることを確認します。



(2) クライアント PC から、Transfer Big Files (<u>https://www.transferbigfiles.com</u>) ヘアクセスすると、拒否されることを確認します。

💋 Applica	tion Blocked ×	30		X
\leftrightarrow \Rightarrow C	● 保護された通信 https://www.transferbigfiles.com	G	☆	:
App Acc Syst Use App	plication Blocked ess to the application you were trying to use has been blocked in accordance with company policy. Please contact y em administrator if you believe this is in error. r: 192.168.45.32 lication: transferbigfiles	our		

(3) a)「Monitor」→ b)「トラフィック」で、ログを確認します。
 アプリケーションの「transferbigfiles」が拒否され、「google-drive-web」が許可されていることがわかります。

■のフォームに c)「(rule eq google-drive-web) or (rule eq Risk5_file-sharing)」と入力して、 ● をクリックすると、 そのルールにヒットしたログだけに絞込み表示されます。

または、「ルール」列の「google-drive-web」と「Risk5_file-sharing」を見つけて、それぞれをクリックすると、国のフォームに自動的に絞込み条件が入ります。ただし、デフォルトは「and」なので、手動で「or」に書き換えてください。

paloalto	_	Dashboard	ACC	Monitor	Policies	Objects	Network	Device					参口ミ	א א 🔓 🕞 Config 🕶	Q.検索
													[手動 💌 😋	のヘルプ
▼@″	Q (n	ule eq google-drive-v	veb) or (n	ule eq Risk5_file-st	naring)									⇒ × ÷	is 🛱 🖗
NG トラフィック 図 登成		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	IP プロトコル	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由	15412
G URL フィルタリング	Þ	03/12 12:33:56	end	Trust	Untrust	192.168.45.32		kix05s01-in-f110.1e100.net	top	443	google-drive-web	allow	google-drive-web	tcp-fin	22.3k
	Ð	03/12 12:33:54	end	Trust	Untrust	192.168.45.32		kix05s01-in-f110.1e100.net	tcp	443	google-drive-web	allow	google-drive-web	tcp-fin	135.3k
□ データ フィルタリング □ HIP マッチ	Þ	03/12 12:33:50	end	Trust	Untrust	192.168.45.32		kix05s07-in-f14.1e100.net	tcp	443	google-drive-web	allow	google-drive-web	top-fin	81.4k
IR ユーザー ID	Þ	03/12 12:33:28	deny	Trust	Untrust	192.168.45.32		tbfweb1.transferbigfiles.com	tcp	443	transferbigfiles	reset-both	Risk5_file-sharing	policy-deny	6.4k
 トンネル検査 説作 	Þ	03/12 12:33:27	deny	Trust	Untrust	192.168.45.32		tbfweb1.transferbigfiles.com	top	443	transferbiofiles	reset-both	Risk5 file-sharing	policy-deny	6.3k

12. Content-ID

Content-ID は、アンチウイルス、脆弱性防御、アンチスパイウェアなど、レイヤ7を検査して脅威を検出する機能です。

以降、それぞれの脅威防御を設定して、比較的容易に実現できる擬似攻撃で、動作を確認します。

12.1.アンチウイルス

ウイルスをブロックする設定を行います。

テスト用ウイルスを提供してくれる eicar サイトヘアクセスして、ウイルスファイルをダウンロードする行為を検知・防御できることを確認します。

12.1.1. 設定前の通信確認

設定前は、ウイルスがダウンロードできてしまうことを確認します。

- (1) クライアント PC で、eicar サイト (<u>http://www.eicar.org/85-0-Download.html</u>) ヘアクセスします。
- (2) HTTP(TCP/80)でダウンロードするウイルスと、HTTPS(TCP/443)でダウンロードするウイルスがあり、それぞれ4種類のファイルが用意されています。

HTTPとHTTPS それぞれ1つ以上ダウンロードできることを確認します。

Download area	a using the standard prot	ocol http	
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes
Download area	a using the secure, SSL en	abled protocol https	
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

※クライアント PC にアンチウイルスソフトウェアがインストールされている場合、そのアンチウイルスが eicar ウイルスを検知し、ダウンロードに失敗したことを示すメッセージが出るかもしれません。

「クライアント PC で検知した」ということは「PA Firewall を通過してクライアント PC まで到達した」ということなので、 PA Firewall のアンチウイルス設定前の動作確認としては、それで OK です。

12.1.2. 設定

(1) a)「Objects」 \rightarrow b)「アンチウイルス」 \rightarrow c)「追加」をクリックします。

paloalto		Dashboard	ACC	Monitor	Polic	ies	Objects	Network	Device			📥 コミット 💣	闷 Config 🗸 🔍 検索
													😋 🕢 ヘルプ
GlobalProtect	٩												1個の項目 🔿 🗙
 ● 小部ダイナミック リスト ▶ ○ カスタム オブジェクト 									デコーダ		7	プリケーション例外	
▼ 図 セキュリティ プロファイル ◎ アンチウイルス b) ラ アンチウイルス b)		名前 🔺	場所		パケッ ト キャプ チャ	名前		アクション		Wildfire アクション	名前	アクション	脅威 例外
・ IBS99 生的 P ローク		default	事前定義法	音み		http		default (reset-both)	allow			0
屆 ファイル プロッキング						smtp		default (alert)		allow			
强 WildFire 分析						imap		default (alert)		allow			
🍅 データ フィルタリング						pop3		default (alert)		allow			
(≢DoS プロテクション						ftp		default (reset-both)	allow			
LS セキュリティ フロファイル グノ						smb		default (reset-both)	allow			
□ク転送 ■ 認証 ▲ 復号プロファイル	(c)											
障碍 スケジュール	÷	追加 🔳 削除	® ⊐ピ–										

(2) a)名前に「AV-Profile01(任意)」と入力します。

デコーダに記載された http プロトコルのアクションが reset-both であることを確認し、c)「OK」をクリックします。 (その他のプロトコルのアクションもどのような設定になっているのか、確認しておいてください。)

7	ンチウイルス プロ	コファイル			0
	名前 AV-F	Profile01	a)		1
	内容				
3	アンチウイルス	ウイルス例外			
	パケット キャプチ・	tr.			
	デコーダ			アプリケーション例外	
١.	デコーダ 🔺	アクション	Wildfire アクション	🔍 0 個の項目s 🔿 🗙	
L.	ftp b	default (reset-both)	default (reset-both)	7	
18	http	default (reset-both)	default (reset-both)	p ===== 2 − 2 − 2 − 2 − 2 − 2 − 2 − 2 − 2	
l	imap	default (alert)	default (alert)	>= yyyy-y=y	
L.	pop3	default (alert)	default (alert)	<u> </u> ソ	
	smb	default (reset-both)	default (reset-both)		
L8	smtp	default (alert)	default (alert)		
				●追加●删除	
				С) ОК + +>セル	

(3) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、プロファイル列 c)「none」をクリックします。

paloalto	D	ashboard ACC	M	lonitor	Policies	Obje	ects N	etwork Devic	e				≜ コミッ	ト 省 🖓 Confiç	g ▼ Q.検 索
															5 ③ヘルプ
■ セキュリティ b)	۹.			_										9個0	の項目s 🗙
å Oos							送信元		*	3 先					
日本 ポリシー ベース フォワーディング		名前	91	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
□ 復号	1	DNS	none	universal	(20) Trust	any	any	any	🕅 Untrust	any	🔝 dns	💥 application-default	⊘ 許可	none	none
▲ トンネル検査 ■ アプリケーション オーパーライド	2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	🗊 ntp	👷 application-default	📀 許可	none	
参認証 ↓ DoS プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	🔆 application-default	🥝 許可	none	
	4	Youtube-other	none	universal	(Dig Trust	any	any	any	(22) Untrust	any	youtube	🙊 application-default	◎ クライアントのリセット	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	google-drive-web	👷 application-default	📀 許可	none	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	(20) Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🚧 Untrust	any	any	🔆 http 🎉 service-https	🥝 許可	^{none} C)	B.
	8	intrazone-default 🧇	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可	none	none
	9	interzone-default 🥎	none	interzone	any	any	any	any	any 💌	any	any	any	◎ 拒否	none	

(4) プルダウンで、「プロファイル」を選択します。

プロファイル		0
プロファイル タイプ	None	•
	プロファイル	
	グループ	
	None	

(5) アンチウイルスで、a)「AV-Profile01」を選択し、b)「OK」をクリックします。

プロファイル	0
プロファイル う	マイプ プロファイル 💌
アンチウイルス	AV-Profile01 a)
脆弱性防御	None
アンチスパイウェア	None
URL フィルタリング	None
ファイル ブロッキ ング	None
データ フィルタリ ング	None
WildFire 分析	None
	b) OK キャンセル

(6) アクション列が「許可」となっているポリシー全てに、同様の方法でアンチウイルスプロファイルを割り当てます。

															5 ()~JUJ
	٩													9個(の項目s 🄿 🗙
NAT QQS ポリシーベースフォワーディング 復号 1 DNS ドンネル検査 アプリケーション オーバーライド 2 NTP							送信元			统				-	
		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔝 dns	💥 application-default	♥許可	-	none	
	none	universal	100 Trust	any	any	any	(22) Untrust	any	iii ntp	👷 application-default	📀 許可	-			
y	ーバーライド 2 NTP 3 Youtube-streaming	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	🕑 許可	3	
	4	Youtube	none	universal	(10) Trust	any	any	any	(22) Untrust	any	youtube	💥 application-default	◎ 拒否	none	B
	5	google-drive-web	none	universal	(20) Trust	апу	any	any	(22) Untrust	any	google-drive-web	👷 application-default	📀 許可	3	
	6	Risk5_file-sharing	none	universal	(22) Trust	апу	any	any	(20) Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	🔮 許可	¢,	
	8	intrazone-default 🔮	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🖸 許可	none	none
	9	Interzone-default	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	B

(7) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

12.1.3. 動作確認

- (1) 再び eicar サイト (<u>http://www.eicar.org/85-0-Download.html</u>) ヘアクセスします。
- (2) HTTPとHTTPSのウイルスそれぞれ1つ以上クリッックしてダウンロードを試みます。

Download are	a using the standard prot	ocol http	
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes
Download are	a using the secure, SSL en	abled protocol https	
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

(3) HTTP(TCP/80)の場合は、PA Firewall から、ブロックされたことが通知されます。
 HTTPS(TCP/443)の場合は、TCP コネクションがリセットされるだけで、通知画面は表示されません(仕様です)。

C 🛈 www.eicar.org/d	iownload/eicar.com	63
Virus/Spyware	Download Blocked	
Virus/Spyware Download of the virus/ believe this is in error.	Download Blocked /spyware has been blocked in accordance with company policy. Please contact your system administrator if you	

(4) a)「Monitor」→ b)「脅威」でウイルスが検知されていることを確認します。

	1	Dashboard	ACC	Monitor	Policies	Objects	Network	Device					813	ミット 💣	🕼 Config 👻 🤇	Q.検索
														手動	S	②ヘルプ
▼ ≧ ⊑ 1'	٩														🖶 🗶 🖶 I	🛱 🏟 🖬
は 同 _{合成} b)		受信日時	タイプ	名前	送信元ゾーン	宛先ゾーン	攻撃者	攻撃者名	被害者	宛先ポート	復号化	アプリケーション	アクション	重大度	ファイル名	URL
URL フィルタリンク	P	03/12 17:11:	29 virus	Eicar Test File	Untrust	Trust	213.211.198.58		192.168.45.32	50032	yes	web-browsing	reset-both	medium	eicar.com	
NildFireへの送信	цр.	03/12 17:10:	27 virus	Eicar Test File	Untrust	Trust	213.211.198.58		192.168.45.32	50028	yes	web-browsing	reset-both	medium	eicar.com	
Image: The second	P	03/12 17:09:	56 virus	Eicar Test File	Untrust	Trust	213.211.198.58		192.168.45.32	50026	yes	web-browsing	reset-both	medium	eicar.com	
国 ユーザー ID	P	03/12 17:09:	49 virus	Eicar Test File	Untrust	Trust	213.211.198.58		192.168.45.32	50024	yes	web-browsing	reset-both	medium	eicar.com	

(5) 上記の c) 🖾のアイコンをクリックすることで、ログの詳細が表示されます。

詳細ログビュ	-											0
全般				送信元	5				宛先			
セッシュ アク アプリケー 仮想シ デバイスのシ IP プロ ログアク 生 受 トンネル	セッション ID 2122 アクション restboth アプリケーション web-browing ルール allow outbound web 仮想システム デバイスのシリアル 番号 P アプロトル tcp ログアクション 生成日時 2018/03/12 17:11:29 トンネル タイプ N/A				攻撃者名 次撃者名 次撃者 マ マ マ マ ボート ゾーン ソ ソ マ	213.211.198. Germany 443 Untrust ethernet1/1 213.211.198. 443 virus Eicar Test File	58		被す す インターフ N NAT 7	書者名 a 皮害者 1 ポート 5 ゾーン 7 ェイス e WAT IP 1 ポート 4	ncmeluser1 192.168.45.32 192.168.0.0-192.168. 50032 Trust athemet1/2 192.168.55.20 11828	255.255
					ID カテゴリ ゲテンツのバーン ジョン度 数し返し回数 ファイル名 URL PCAP ID 送信元 UUID 宛先 UUID	90826973 (Vi js Antivirus-576 medium 1 eicar.com 0	ew in Thre	at Vault)	フラグ キャプティフ プロキシト クラ パケット = クライアン サーバーから トンネル検到	f デジ 复 キ トー クア 査済 ポタ ンヨ 号 ャチ かバ ラン 済み レガン 化 プヤ らー イト み		
				電子メ	【ール ヘッダ 諸のアドレス サブジェクト							
PCAP 受信日時 2018/03	12 17:11:37	タイプ end	アプリケ ン web-brow	ーショ wsing	アクション allow	ルール allow outbound	バイト 5587	重大度	カテゴリ computer- and-internet-	判定	URL	ファイル名
2018/03	12 17:11:29	virus	web-brow	wsing	reset-both	allow outbound web		medium	info computer- and-internet- info			eicar.com
												閉じる

※ログの確認ポイントや、検知以降の実施 すべきアクション等は、別途発行している 「PA Series Firewall 運用ガイド」 をご参照ください。

12.2. 脆弱性防御

脆弱性防御の設定を行います。

脆弱性防御シグネチャの中に、「クロスサイトスクリプティング」攻撃に関するシグネチャが存在しています。 この攻撃が模擬しやすいので、動作確認にはこの攻撃を使います。

12.2.1. 設定

(1) a)「Objects」 \rightarrow b)「脆弱性防御」 \rightarrow c)「追加」をクリックします。

paloalto		Dashb	oard AC	C N	Ionitor	Policies	Objects	Network	Device			🏝 コミット 🧉 (🖉 Config 🔻 🔍 検索
													😋 🔞 ヘルプ
💷 アプリケーション グループ	٩												2 個の項目s 🗎
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		名前	場所	カウント	ルール名		脅威名	ホスト タイプ	重大度	アクション	パケット キャプチャ		
サービス グループ		strict	事前定義済み	ルール: 10	simple-client	-critical	any	client	critical	reset-both	disable		
8 9 17					simple-client	t-high	any	client	high	reset-both	disable		
GlobalProtect					simple-client	-medium	any	client	medium	reset-both	disable		
● 外部ダイナミック リスト					simple-client	-informational	any	client	informational	default	disable		
					simple-client	-low	any	client	low	default	disable		
▼ ③ ゼキュリティ ノロノアイル ▲ マンチウノルフ					simple-serve	er-critical	any	server	critical	reset-both	disable		
					simple-serve	er-high	any	server	high	reset-both	disable		
● 脆弱性防御 b)	1				詳細								
URL フィルタリング		default	事前定義済み	ルール: 6	simple-client	-critical	any	client	critical	default	disable		
📑 ファイル ブロッキング					simple-client	t-high	any	client	high	default	disable		
📑 WildFire 分析					simple-client	-medium	any	client	medium	default	disable		
🚵 データ フィルタリング					simple-serve	er-critical	any	server	critical	default	disable		
建DoS プロテクション					simple-serve	er-high	any	server	high	default	disable		
セギュリティ プロファイル グノ					simple-serve	er-medium	any	server	medium	default	disable		
「 復長プロファイル		-											
■ スケジュール		C)											
	ŧ	追加	- 削除 👩 コピ										

(2) 重大度が高い場合にはパケットキャプチャを実施する、というルールを生成することにします。a)名前に「VP-Profile01(任意)」と入力し、b)「追加」をクリックします。

脆弱性防御	卸プロフ	アイル					0 🗖
	名前 VP	-Profile01	a)				
	内容						
ルール	例外						
ע-גו	儿名	脅威名	CVE	ホスト タイプ	重大度	アクション	パケット キャプ チャ
b)	1						
🕂 追加	∋削除(3 ±∧ ♥ ™∧	💿 コピー 🔍 一致する:	シグネチャを検出			
						ок	キャンセル

(3) a)名前に「VP-Rule01(任意)」と入力し、b)パケットキャプチャは「extended-capture」を選択します。
 c)の重大度は「critical」と「high」にチェックを入れて、d)「OK」をクリックします。

脆弱性防御川	レール			0	
ルール名	VP-Rule01	a)			
脅威名	any				
アクション	シグネチャ名の一部として入 デフォルト	カされたテキストを含むすべてのシグネチャの	D照合(i ▼	に使用 パケット キャ extended-capture ▼ プチャ	b)
ホスト タイプ	any		-	カテゴリ any 💌	
🗹 いずれか		🗹 いずれか		重大度	
CVE 🛦		ペンダー ID ▲		any (All severities) critical high medium low informational	
🕂 追加 🕒 🏻	川除	● 追加 ● 削除			
シグネチャ CVE また	はペンダー ID の一部としてフ	力されたテキストを含むすべてのシグネチャ	の照合	に使用	
				d) ок <i>キャンセル</i>	

(4) 再度「追加」をクリックし、a)名前に「VP-Rule02(任意)」と入力し、b)パケットキャプチャは「disable」を選択します。
 c)の重大度は「medium」と「low」と「informational」にチェックを入れて、d)「OK」をクリックします。



(5) 「OK」をクリックします。

脆弱性防御プロ	ファイル					(0 🗉
名前	VP-Profile01						
内容							
ルール 例外							
■ ルール名	脅威名	CVE	ホスト タイプ	重大度	アクション	パケット キャプチャ	
VP-Rule01	any	any	any	critical high	default	extended-capture	
VP-Rule02	any	any	any	medium Iow informational	default	disable	
🕂 追加 🕒 削除	 ・ ・	🌀 그 ピー 🔍 — 🕱	なするシグネチャを検出				
						OK キャンセ/	v

(6) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、c)プロファイル列にあるアイコン をクリックします。

NETWORKS	U	ashboard ACC	N	Ionitor	Policies	Obje	cts N	etwork Devic	e				@ _ < y		」▼ ~ 使米
															S 0~
ztaufr b)	٩													9個(の項目s 🏓
							送信元		1	统					
シー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
1 10.00	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	📰 dns	👷 application-default	📀 許可	-	none
- ンネル検査 ? プリケーション オーバーライド 8証 IoS プロテクション	2	NTP	none	universal	(20) Trust	any	any	any	(22) Untrust	any	🗊 ntp	👷 application-default	😕 許可	-	•
	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	(20) Untrust	any	youtube-base	\chi application-default	😋 許可		
	4	Youtube-other	none	universal	(20) Trust	any	any	any	(22) Untrust	any	j youtube	👷 application-default	◎ クライアントのリセット	none	
	5	google-drive-web	none	universal	() Trust	any	any	any	(22) Untrust	any	google-drive-web	👷 application-default	📀 許可	4	
	6	Risk5_file-sharing	none	universal	(10) Trust	any	апу	any	🕅 Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	апу	any	(22) Untrust	any	any	🔆 http 🔆 service-https	🥴 許可	🤹 c)	
	8	intrazone-default 🛛 🎯	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可	none	none
	9	interzone-default	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(7) a)「脆弱性防御」で、a)「VP-Profile01」を選択し、b)「OK」をクリックします。

プロファイル		0
プロファイル う	イプ プロファイル	•
アンチウイルス	AV-Profile01	~
脆弱性防御	VP-Profile01 a)	~
アンチスパイウェア	None	~
URL フィルタリング	None	~
ファイル ブロッキ ング	None	~
データ フィルタリ ング	None	~
WildFire 分析	None	~
	b) OK キャンセル	

(8) アクション列が「許可」となっているポリシー全てに、同様の方法で脆弱性防御プロファイルを割り当てます。

															S ()~167
■ セキュリティ	٩,													9個	の項目s 🔿 🕽
♦ NAT QoS							送信元			洗					
● cus ● ポリシー ベース フォワーディング ● 復号 ● トンネル検査 ■ アプリケーション オーバーライド		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	апу	any	(22) Untrust	any	🔝 dns	👷 application-default	許可	Q. J	none
	2	NTP	none	universal	fill Trust	any	any	any	(22) Untrust	any	🛄 ntp	💥 application-default	📀 許可	Ø.J	
いたい ション・ハーン・ハーン・ハーン・ハーン・ハーン・ハーン・ハーン・ハーン・ハーン・ハー	3	Youtube-streaming	none	universal	(100) Trust	апу	апу	any	🕅 Untrust	any	youtube-base	💥 application-default	🕲 許可	3 3	
	4	Youtube	none	universal	(22) Trust	any	any	any	(22) Unbrust	any	j youtube	× application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	google-drive-web	👷 application-default	📀 許可	3 .	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	(22) Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	2 http 2 service-https	🕗 許可	4 7	
	8	intrazone-default 🧇	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🖸 許可	none	none
	9	interzone-default 🧐	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	ED)

(9) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

クロスサイトスクリプティング攻撃を模擬します。

(1) 入力フォームを持つサイト (例:<u>https://www.google.co.jp</u>) で、以下の文字列を入力し、送信します。

<script>alert(XSS Test)</script>

	Google												
<script>alert(XSS</th><th>Fest)</script>													
	Google 検秦 I'm Feeling Lucky												
	Google が提供: E	nglish											

(2) a)「Monitor」→ b)「脅威」でログを確認します。 以下のように、タイプが「Vulnerability (脆弱性)」として検知した脅威ログが出力されます。

paloalto	Dashboard	ACC	Monitor	Policies Obje	ts Network	Device					<u>*</u> :	コミット 🗳	闷 Config	▼ Q.検索
												手動	_ 2	3 ②ヘルプ
マログ	۹.			_									😑 🗙 🗄	i 🛱 🎇 🚳
	受信日時	タイプ	名前		送信元ゾーン	宛先ゾーン	送信元アドレス	送信元ユーザー	宛先アドレス	宛先ポート	アプリケーション	アクション	重大度	ファイル名
ORE 74703 777	504/01 11:2	8:59 vulnerabi	lity Generic H	TTP Cross Site Scripting Atte	mpt Trust	Untrust	192.168.45.32		172.217.161.227	443	google-base	alert	high	www.google.c
MildFireへの送信		. L												

- (3) ログの先頭から2つ目の。アイコンをクリックすると、パケットキャプチャデータがダウンロードできます。
- ※ v8.1.0 では、上記の↓をクリックしても「File not found」と表示される不具合が存在します。(v8.1.1 で修正予定。) 代替策として、以下の「詳細ログビュー」の下方に表示される関連ログの↓をクリックすることで取得できます。
- (4) ログの先頭の アイコンをクリックすることで、詳細ログを確認できます。

設				送信	元				宛先					
セッション ID	2722			ž	5信元ユーザー				宛先ユー	ザー				
アクション	alert				送信元	192.168.45.32			1	宛先 17	2.217.16	1.227		
アプリケーション	google-base				1	192.168.0.0-192.3	168.255.25	5		街 Ur	nited Stat	es		
ルール	allow outbound web				ポート	50340			ボ・	ート 44	3			
仮想システム					ゾーン	Trust			ゾーン Untrust					
デバイスのシリアル				13	<i>νター</i> フェイス	ethernet1/2			インターフェイス ethernet1/1					
111 プロトコル	ten				NAT IP	192.168.55.20			NA	T IP 17	2.217.16	1.227		
ログアクション	tep				NAT ポート	64516			NAT ポ・	-ト 44	3			
生成日時	2018/04/01 11:28:59													
受信日時	2018/04/01 11:28:59			詳細										
トンネル タイプ	N/A													
					背威タイプ	vulnerability								
					背旗名	Generic HTTP Cro	ss Site Scri	oting Attempt						
					10	314/7 (View in Tr	reat vauit							
					カナコウ (テンパのパー	code-execution								
					ジョン	AppThreat-797-46	514		フラグ					
					重大度	high			キャプティブ・					
					繰り返し回数	1			477747					
						www.google.co.jp q= <script>alert() oq=<script>alert() </script> &gs_l=p ab.30.0.0.20939	/search?ei (SS%20Tes (XSS%20Te (SS%20Te (SS%20Te (SS%20Te (SS%20Te) (SS%20Te	=1UPAWt7c t)& st) 0.0.00.0	プロキシ トラ クシ 復	ンザ ヨン 号化 マ	2			
						ab0.0.00.9UR	-eZdCsXE		パケットキ	ヤノチャ 💽				
					URL				クライアント:	0.6 L	2			
					PCAP ID	12040097938412	56692		サー.	/<- 🖻				
					送信元 UUID				サーバーからク	ジレ [
					宛先 UUID				トンネル検査	済み				
				電子 . 送信	メ ール ヘッダ 諸のアドレス サブジェクト	1								
? 受信日時 ▲	タイプ		アプリケー	ション	アクション	ルール	パイト	重大皮	カテゴリ	判定		URL	ファイル名	
2018/04/01 11:2	18:59 url		google-bas	e	alert	allow outbound web		informational	search- engines			www.google		
2018/04/01 11:2	18:59 vulnerab	oility	google-bas	e	alert	allow outbound web		high	search-				www.google	

※ログの確認ポイントや、検知以降 の実施すべきアクション等は、別途発 行している 「PA Series Firewall 運用ガイド」 をご参照ください。 Wildfire クラウド(サンドボックス)が、未知*の攻撃を検知できるように設定します。

動作確認には、パロアルトネットワークス社が提供するテスト用の未知ウイルスをダウンロードし、それを検知することを確認します。

「未知」とは:「アンチウイルス」シグネチャにヒットするものが「既知」で、それにヒットしないものが「未知」という扱いです。 未知のファイルの中にも無害なものと有害なものが存在し、WildFire で有害と判定されるものが「未知ウイルス」です。

12.3.1. 設定

(1) a)「Objects」→ b)「Wildfire 分析」→ c)「追加」をクリックします。

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device			≜ コミット	< 🧉 阔 Cor	fig ▼ ♀ 検索
													😋 🕢 ヘルプ
▽ 🗷 セキュリティ プロファイル												1	個の項目 🌛 🗙
アンチウイルス		名前		場所		ルール名		アプリケーショ	עו	ファイル タイプ		方向	分析
▶ 脆弱性防御		default		事前定義済み		default		any		any		both	public-cloud
GURL フィルタリング													
🖳 WildFire 分析 b)	1												
EDoS プロテクション													
セキュリティ プロファイル ら 口グ転送		c)											
	Ð	追加 🖃 削除 💿	⊐Ľ–										

(2) a)名前に「WF-Profile01(任意)」と入力し、b)「追加」をクリックします。
 c)名前に「All-files(任意)」と入力し、d)「OK」をクリックします。

WildFire 分析プロファイル			0
名前 WF-Profile01 a) 内容			
٩			1 個の項目 🔿 🗙
名前 アプリケーション	ファイル タイプ	方向	分析
All-files C any	any	both	public-cloud
b)			
登 追加			
		d)	OK キャンセル

(3) SSL 復号化を行なっている場合には、以下の設定も必要です。

a)「Device」 → b)「セットアップ」 → c)「コンテンツ ID」で表示された「コンテンツ ID 設定」の d) ^並アイコンをクリックします。

paloalto	Dashboard ACC Monitor Policies Objects Network Device	👗 コミット 省 🖓 Config - 🤇 検索
	a)	S ()~1/7
 	管理 操作 サービス インターフェイス テレメトリー コンテンツID	WildFire セッション HSM
№ 設定監査	URL フィルタリング C) 🟚	コンテンツID 設定 d) 🌣
5 管理者	ダイナミック URL キャッシュのタイムアウト (時間) 168	復号化されたコンテンツの転送を許可
② 管理者ロール ③ 認証プロファイル	URL コンティニュー タイムアウト (分) 1	拡張パケット キャプチャ長 (パケット数) 5
2 認証シーケンス	URL 管理オーバーライド タイムアウト (分) 15	TCP App-ID検査キューを超過したセグメントを転送
III ユーザー ID	URL 管理ロックアウト タイムアウト (分) 30	TCPコンテンツ検査キューを超過したセグメントを転送 📝
 WM 情報ソース マ 同 証明書の管理 	PAN-DB サーバー	UDPコンテンツ検査キューを超過したデータグラムを転送 √
2 証明書		HTTPの部分的な応答を許可 🧹
📮 証明書プロファイル	upl 飾理ナーパーニノド	

(4) a)「復号化されたコンテンツの転送を許可」にチェックを入れ、b)「OK」をクリックします。



(5) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、c)プロファイル列にあるアイコン をクリックします。

paloalto	1	Dashboard ACC		Monitor	Policie	es Ob	jects	Network Dev	ice				🍰 コミッ	ト 💣 🔯 Config	g▼ Q 検索
															S ()~117
■セキュリティ b)	٩,													9個(の項目s 🔿 🗙
Se NAT							送信元		5	动物		1			line in
日本 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔟 dns	💥 application-default	於可	0	none
(▲トンネル検査 ■ アプリケーション オーバーライド 参 認証 ■ DoS プロテクション	2	NTP	none	universal	(10) Trust	any	any	any	(27) Untrust	any	mtp	👷 application-default	📀 許可	3 3	
	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	X application-default	📀 許可	Ø J	
	4	Youtube	none	universal	(22) Trust	any	any	any	🙀 Untrust	any	youtube	× application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	google-drive-web	👷 application-default	📀 許可	3 3	B
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	(22) Untrust	any	😽 Risk5_file-sharing	👷 application-default	◎ 拒否	none	B
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	🗶 http 🗶 service-https	🕑 許可	🌌 C)	
	8	intrazone-default 🔮	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可	none	none
	9	interzone-default 🥎	none	interzone	any	any	any	any	any	any	апу	any	◎ 拒否	none	

(6) a)「WildFire 分析」で、a)「WF-Profile01」を選択し、b)「OK」をクリックします。

プロファイル	0
プロファイル う	マイプ プロファイル
アンチウイルス	AV-Profile01
脆弱性防御	VP-Profile01
アンチスパイウェア	None
URL フィルタリング	None
ファイル ブロッキ ング	None
データ フィルタリ ング	None
WildFire 分析	WF-Profile01 a)
	b) ок т +v>セル

(7) アクション列が「許可」となっているポリシー全てに、同様の方法でWildFire プロファイルを割り当てます。

paloalto	1	Dashboard ACC		Monitor	Policie	es Ob	jects	Network Dev	ice				🍰 コミッ	ト 💣 😡 Confi	g ▼ Q.検 索
															5 ②ヘルプ
🕮 セキュリティ	۹.													9 個	の項目s 📑 🗙
PNAT							送信元			3先					
曝ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
· 復号	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🛄 dns	💥 application-default	🙂 許可	8 V A	none
 トンネル検査 アプリケーション オーパーライド 	2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	апу	mtp	👷 application-default	🔮 許可	80 R	
 2000 アロテクション 	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	M Untrust	any	youtube-base	💥 application-default	🕑 許可	Ø J 🔒	
	4	Youtube	none	universal	(iii) Trust	any	any	any	(22) Untrust	any	youtube	💥 application-default	◎ 拒否	none	B
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	google-drive-web	× application-default	📀 許可	80 R	
	6	RiskS_file-sharing	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	B
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	 http service-https 	🕑 許可	8 J 🔒	
	8	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🖸 許可	none	none
	9	interzone-default 🏀	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(8) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
12.3.2. 動作確認

(1) クライアントから、以下 Link ヘアクセスして、テスト用の未知マルウエアファイルをダウンロードします。

http://wildfire.paloaltonetworks.com/publicapi/test/pe

(HTTPS サイトで確認したいところですが、「*.wildfire.paloaltonetworks.com」サイトへの通信はデフォルトで「SSL 復号化 除外」となっています。よって、HTTP(暗号化なし)で動作確認を行なってください。)

(2) CLI コマンドで、ファイル転送のカウントが Up していることを確認します。

admin@PA-VM> show wildfire status

Connection info:	
Signature verification:	enable
Server selection:	enable
File cache:	enable
WildFire Public Cloud:	
Server address:	wildfire.paloaltonetworks.com
Best server:	panos.wildfire.paloaltonetworks.com
Device registered:	yes
Through a proxy:	no
Valid wildfire license:	yes
Service route IP address:	192. 168. 45. 11

~略~

Forwarding info:	
file idle time out (second):	90
total concurrent files:	0
Public Cloud:	
total file fwded :	1
total file failed:	0
total file skipped:	0
total cloud queries:	1
total cloud queries failed:	0
file forwarded in last minute:	0
concurrent files:	0

~略~

(3) 10 分程度待ちます。

(※Wildfire クラウドでの解析に 5~10 分かかるので、ログ出力されるのも、5~10 分かかります。)

(4) a)「Monitor」→ b)「WildFire への送信」でログを確認します。
 以下のように、判定が「Malicious」として検知したログが出力されます。

paloalto		Dashboard	ACC Mon	itor	Policies	Objects	Network	Device					舎コミッ	y k 💣 😡 G	onfig 🗝 🔍
													1	手動	- S 🛛
▼ 🔁 ログ	۹.													-	× 🕂 👦
N トラフィック 図 音威		受信日時	ファイル名	URL	送信元ゾーン	宛先ゾーン	攻撃者	攻撃者名	被害者	宛先ポート	アプリケーション	ルール	判定	アクション	重大度
URL 74707927	Þ	02/08 12:15:08	wildfire-test-pe-file.exe		Untrust	Trust	52.193.2.75		192.168.45.32	58331	web-browsing	allow outbound web	malicious	allow	high
WildFireへの送信 D															
■ J = 9 J + 709 9 J 9 ■ HIP マッチ															

(5) ログの先頭の『シアイコンをクリックすることで、詳細ログを確認できます。

詳細ログ ビュー										0 🗖
ログ情報 WildFi	ire 分析レポート									
全般		送信	元				宛先			
セッション ID アクション アプリケーション ルール 判定 仮想システム デバイスのシリアム 番号	61300 allow web-browsing allow outbound web malicious 015351000008994	4	攻撃者4 攻撃者 ポート ゾーン ンターフェイン NAT I NAT ポート	名 52.193. ト 80 ン Untrust ス etherne P ト 80	2.75 t1/1		インター	被害者名 被害者 ポート ゾーン フェイス NAT IP T ポート	192.168.45.3 58331 Trust ethernet1/2 31246	2
ログ アクション 生成日時 受信日時 トンネル タイプ	2018/02/08 12:15:08 2018/02/08 12:15:08 N/A	詳細					フラグ キャプテ・	ィブポー		_
HTTP ヘッダー		脅威	な な コンテンツ タ イラ	タ プ wildfire			プロキシ	タル トランザ		
ユーザー エージェ ント Referrer X-Forwarded-For			ID 8427870856 重大皮 high 繰り返し回数 1 ファイルタイプ pe					クション 復号化 ト キャプ チャ ントから		
電子メール ヘッタ	1		ファイル名 wildfire-test-pe-file.exe URL					サーバー らクライ アント	v	
送信者のアドレス 受信者のアドレス 受信者のユーザー ID サブジェクト							トンネル	検査済み		
PCAP 受信日時 🔺	タイプ	アプリケー ション	アクショ ン	ルール	パイト	重大度	カテゴリ	判定	URL	ファイル 名
2018/02/08 12:09:24	end v	web-browsing	allow	allow outbound web	59850		computer- and- internet- info			
2018/02/08 12:15:08	wildfire v	web-browsing	allow	allow outbound web		high		malicious	5	wildfire
			_							閉じる

(6) 「Wildfire 分析レポート」タブをクリックすると、なぜこのファイルがウイルスと判定されたのかの詳細を確認することが できます。

詳細口	コグビュー										Ø			
ログ	情報 WildFi	ire 分析レポート	•											
Wild	Fire Analys	sis Summary								Down	nload PDF			
File 1	Information													
File T	ype	PE												
File S	igner													
SHA-2	256	72a4119e	2a4119eea2a9dab316ff8c40ad89f9e509c2e967be1f8693b17da077478e110											
SHA1		0efc2dd8b	2fc2dd8b65d4954e7c0784244cfe8557d57fc9a											
MD5		9338493d	500351c67dca0bc	94a2ddf02										
File S	ize	55296 byt	es											
First S	Seen Timestamp	2018-02-0	8 03:09:04 UTC											
Verdia	ct	malware												
Samp	Sample File Download File													
For en	erage Statu adpoint anti-virus 受信日時 ▲	25 coverage informati タイプ	ion for this sample	, visit Virus アクショ	Total	パイト	重大度	カテゴリ	判定	URL	77-11	īμ		
		14	עובע	9							看			
	2018/02/08 12:09:24	end	web-browsing	allow	allow outbound web	59850		computer- and- internet- info						
	2018/02/08 12:15:08	wildfire	web-browsing	allow	allow outbound web		high		malicious		wildfire	•		
											閉じる			

※ログ内容の確認方法や、検知以降の 実施すべきアクション等は、別途発行し ている「PA Series Firewall 運用ガイ ド」をご参照ください。 ファイルブロッキング機能を使うことで、ファイル種別をファイルヘッダで判別し、許可・拒否などの制御を行うことができます。

以下の要件を想定した設定を行います。

「XXX.exe ファイルなどの PE (Portable Executable)* を全てブロックすると業務に支障が出るので、ダウンロード時は 警告を出すが、ダウンロードするかどうかはユーザ判断とする。」

[PE (Portable Executable)]: 主に Microsoft Windows 上で使用される実行ファイルフォーマットのこと。

12.4.1. 設定

(1) a)「Objects」→ b)「ファイル ブロッキング」で表示された c)「basic file blocking」を選択した状態で、
 d)「コピー」をクリックします。

paloalto		Dashboard	ACC	Monitor	Policies	Obiects	Network	Device	≛ ⊐	ミット 윱 (Config ▼ Q 検索
						a)					5 ③ヘルプ
<mark>.</mark> ♥ URL カテゴリ	٩										2 個の項目s 🔁 🗙
▼ × セキュリティ プロファイル		名前	場所 🔺	ルール名		アプリ ケーショ ン	ファイル タイ	プ		方向	アクション
● 肥弱性防御		basic file blocking	事前定義済み	Block high ris	sk file types	any	7z, bat, chm,	class, cpl, dll, exe	, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
「ファイル ブロッキング b)				Continue pro	ompt encrypted files	any	encrypted-rar,	encrypted-zip		both	continue
WildFire 2MT	4	0)		Log all other	file types	any	any			both	alert
🏠 データ フィルタリング		strict file blocking	事前定義済み	Block all risk	y file types	any	7z, bat, cab, c PE, pif, rar, sci	hm, class, cpl, dll ; tar, torrent, vbe,	, exe, flash, hlp, hta, msi, Multi-Level-Encoding, ocx, , wsf	both	block
■ DoS プロテクション				Continue pro	mpt encrypted files	any	encrypted-rar,	encrypted-zip		both	block
■ ログロング				Log all other	file types	any	any			both	alert
10 四元			d)								
Cititi poal.	÷	追加 🖃 削除 📀	コピ ー								

(2) 「OK」をクリックします。

⊐ピ –	Ø
選択済み オプジェ クト	名前 basic file blocking
	√ 検証で最初に検出されたエラーに起因するエラーが発生しました
	OK キャンセル

(3) $\exists l' = \delta h t$ basic file blocking-1] δp blocking-1] δp

paloalto		Dashboard	ACC	Monitor F	Policies	Objects	Network	Device	\$	コミット 💣	闷 Config ▾ 🔍 検索
											😋 💿 ヘルプ
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	٩										3 個の項目s 🕇 🗙
● URL カテゴリ ▼ 図 セキュリティ プロファイル ◎ アンチウイルス		名前	場所 🔺	ルール名		アプリ ケーショ ン	ファイル タイ	7		方向	アクション
アンチスパイウェア ● 脆弱性防御 『 リローマム クリング		basic file blocking-1		Block high risk fi Continue prompt	ile types t encrypted files	any any	7z, bat, chm, encrypted-rar,	class, cpl, dll, exe encrypted-zip	, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, w	f both both	block continue
● URL フィルダリンク ■ ファイル プロッキング ■ WildFire 分析	4	basic file blocking	事前定義済み	Log all other file Block high risk fi Continue prompt	types ile types t encrypted files	any any any	any 7z, bat, chm, encrypted-rar,	class, cpl, dll, exe encrypted-zip	, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, w	if both both	alert block continue
illist データ フィルタリング ■ DoS プロテクション		strict file blocking	車前定義済み	Log all other file Block all risky file	e types	any	any 7z bat cab o	hm class col dil	eve flach bin hta msi Multi-Level-Encoding o	both	alert
10 セキュリティ プロファイル グノ 国 ログ転送		Solice the blocking		Continue prompt	t encrypted files	any	PE, pif, rar, sc encrypted-rar,	encrypted-zip	WSF	both	block
■ 認証				Log all other file	types	any	any			both	alert
囲 スケジュール	÷	追加 🖃 削除 👩	コピ ー								

(4) 名前をa)「FB-Profile01(任意)」に変更します。

「Block high risk file types」行のファイルタイプから、PE と exe を削除します。 その行のファイルタイプをクリックして、a) exe と PE にチェックを入れて、b)「削除」をクリックします。

ファイル ブロッキ	ングプロファイル				0
名前 FB-	Profile01 C)				
内容				3個の道日。	
■ 名前	アプリケーション	ファイル タイプ	方向	アクション	
Block high risk file types	any	Uvg*nか v exce hlp hta jar a) ocx V PE ◆ 注加 ●別廠 b)	both	block	
🕂 追加 🖃 削除			10- 		
					・ンセル

(5)「Continue prompt encrypted files」行のファイルタイプに、PEと exe を追加します。
 その行のファイルタイプをクリックして、a)「追加」をクリックして、b)PEと exe を選択します。
 c)「OK」をクリックします。

ファイル ブロッキン	ノグ プロファイル			0
名前 FB-F	Profile01			
内容				
۹.				3 個の項目s 🗙
🔲 名前	アプリケーション	ファイル タイプ	方向	アクション
		rar scr torrent vbe		
Continue prompt encrypted files	any	いずれか encrypted-rar	both	continue
Log all other file types	any	PE b)	both	alert
🕂 追加 🖃 削除		exe D7		
	e	2) 于追加 ■ 削除	c) [OKキャンセル

(6) FB-Profile01のファイルタイプは、以下の状態になります。

名前	Ũ	場所 🔺	ルール名	アプリケー ション	ファイル タイプ	方向	アクション
FB-P	Profile01		Block high risk file types	any	7z, bat, chm, class, cpl, dll, hlp, hta, jar, ocx, pif, rar, scr, torrent, vbe, wsf	both	block
			Continue prompt encrypted files	any	encrypted-rar, encrypted-zip, exe, PE	both	continue
			Log all other file types	any	any	both	alert

(7) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、c)プロファイル列にあるアイコン をクリックします。

paloalto	1	Dashboard ACC		Monitor	Policie	es Ob	ojects	Network Dev	се				🍰 コミッ	ト 🧉 🖓 Config	▼ Q.検索		
														1	3 ⑦ヘルナ		
■セキュリティ b)	٩													9 個の)項目s 🔿 🗙		
🐨 NAT							送信元			8先							
曝 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション		
	1	DNS	none	universal	(20) Trust	any	any	any	🕅 Untrust	any	dns	👷 application-default	⊘ 許可	80 a	none		
トンネル検査 アプリケーション オーバーライド	2	3	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	mtp	👷 application-default	🔮 許可	80 B	
 				3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	🗶 application-default	🕑 許可	Ø J 🔒
	4	Youtube	none	universal	(20) Trust	any	any	any	🕅 Untrust	any	j youtube	🙊 application-default	◎ 拒否	none			
	5	google-drive-web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	google-drive-web	👷 application-default	📀 許可	Ø			
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	🚧 Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none			
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	🔆 http 🎉 service-https	🕑 許可	⊘ 0 ⊾ C)	B		
	8	intrazone-default 🚳	none	intrazone	any 💌	any	any	any	(intrazone)	any	any	any	◎ 許可	none	none		
	9	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none			

(8) a)「ファイルブロッキング」で、a)「FB-Profile01」を選択し、b)「OK」をクリックします。

プロファイル		0
プロファイル タ	イプ プロファイル	~
アンチウイルス	AV-Profile01	-
脆弱性防御	VP-Profile01	-
アンチスパイウェア	None	-
URL フィルタリング	None	-
ファイル ブロッキ	FB-Profile01 a)	•
ジッ・ データ フィルタリ ング	None	•
WildFire 分析	WF-Profile01	•
	b) ок <i>тту</i>	L)

(9) アクション列が「許可」となっているポリシー全てに、同様の方法でファイルブロッキングプロファイルを割り当てます。

paloalto	1	Dashboard ACC		Monitor	Policie	s Ob	jects	Network Dev	ce				≛ コミッ	ト 🧉 阔 Config	▼ Q.検索
															ロ ②ヘルプ
📟 セキュリティ	9													9個0	項目s 🔿 🗙
TAN							送信元		5	统					
します。 マック・マース フォワーディング		名前	97	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
◎ 復号	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔝 dns	🔆 application-default	🕑 許可	Ø	none
 トンネル検査 アプリケーション オーバーライド 	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🛄 ntp	👷 application-default	🕑 許可	80 B B	
● 認証 ● DoS プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	(129) Untrust	any	youtube-base	🔆 application-default	🕑 許可	80	
	4	Youtube	none	universal	🕅 Trust	any	any	any	🕅 Untrust	any	youtube	👷 application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	google-drive-web	👷 application-default	🔮 許可	806a	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	💥 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	http service-https	🕑 許可	80 B	
	8	intrazone-default 🥹	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🖸 許可	none	none
	9	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(10)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

12.4.2. 動作確認

(1) クライアント PC の Web ブラウザから以下へアクセスして、PE ファイル (exe ファイル) をダウンロードします。

http://wildfire.paloaltonetworks.com/publicapi/test/pe

(2) 以下のような、「Continue」ボタン付きの警告画面が表示されます。

「Continue」をクリックすると、ダウンロードが始まります。

	ile Download Blocked ×	
<	C 🛈 wildfire.paloaltonetworks.com/publicapi/test/pe	⊠ ☆ :
	File Download Blocked	
	Access to the file you were trying to download has been blocked in accordance with compa contact your system administrator if you believe this is in error.	ny policy. Please
	File name: wildfire-test-pe-file.exe	
	Please clicit Continue to download/upload the file.	

(3) a)「Monitor」 → b)「データ フィルタリング」でログを確認します。

まず、アクションが「block-continue」のログが出力され、Continue ボタンが押されてダウンロードが実施された場合には、アクションが「Continue」のログが出力されます。

paloalto		Dashboard J	ACC Monitor	Policies Obje	ts	Network Device						8	コミット 省 ಢ	Config - 9、検索
			a)										f£	- C O~-
V Car														x @ = # *
■ トラフィック □		受信日時	カデゴリ	ファイルモ	URL	名的	送信元ゾーン	和先ゾーン	送信者	送信者名	20.6	和先ポート	アプリケーション	79382
La URL フィルタリング	ID.	03/17 15:38:14	computer-and-internet-info	wildfire-test-pe-file.exe		Windows Executable (EVE)	Untrust	Trust	ec2-52-193-2-75.ap-northeast-1.compute.amazonaws.com		192.168.45.32	49736	web-browsing	continue
マータフィルタリング b		03/17 15:38:12	computer-and-internet-info	wildfre-test-pe-file.exe		Microsoft PE File	Untrust	Trust	ec2-52-193-2-75.ap-northeast-1.compute.amazonaws.com		192.168.45.32	49735	web-browsing	block-continue

12.5.アンチスパイウェア

アンチスパイウェア機能には2つの防御シグネチャが存在します。

ーつ目は、スパイウェアが使うコマンド&コントロール(C2)サーバーへの通信を検出する C2 シグネチャ、二つ目は、C2 サイトへの DNS クエリを検出する DNS シグネチャです。

C2 シグネチャにヒットする攻撃を模擬するのは難しいので、DNS シグネチャにヒットする攻撃を模擬して、DNS シンクホール*が動作することを確認します。

[DNS シンクホール]: クライアントからマルウェアサイトへの DNS リクエストが発せられた場合に、PA Firewall は、あらかじめ設定された偽りの IP アドレスを DNS レスポンスに入れて返答する機能のことです。

12.5.1. 設定

(1) a)「Objects」 \rightarrow b)「アンチスパイウェア」 \rightarrow c)「追加」をクリックします。

paloalto		Das	nboard A	.00	Monitor Polic	ies	Objects	Network	Device		
							a)				
い アドレス クループ		名前	場所	カウント	ルール名	脅威名	重大度	アクション	パケット キャプチャ	DNS パケット キャプチャ	
□ アプリケーション		default	事前定義済み	ルール: 4	simple-critical	any	critical	default	disable	disable	
🛅 アプリケーション グループ					simple-high	any	high	default	disable		
🖙 アプリケーション フィルタ					simple-medium	any	medium	default	disable		
					simple-low	any	low	default	disable		
N 9-EX 9/0-7		strict	事前定義済み	ルール: 5	simple-critical	any	critical	reset-both	disable	disable	
➢ GlobalProtect					simple-high	any	high	reset-both	disable		
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●					simple-medium	any	medium	reset-both	disable		
▶ 👵 カスタム オブジェクト	4				simple-informational	any	informational	default	disable		
▽ 🗷 セキュリティ プロファイル	1				simple-low	any	low	default	disable		
2 アンチウイルス											
\mathcal{D} \mathcal{D} \mathcal{D} \mathcal{D}											
B ファイル ブロッキング											
WildFire 分析											
📥 データ フィルタリング		\sim									
€ DoS プロテクション				, <u> </u>							
	÷		- 別际 🌀 コヒ								

(2) a)名前に「AS-Profile01(任意)」と入力し、b)「追加」をクリックします。

アンチスパイウェア	^ア プロファイル			0
名前	AS-profile01	a)		
内容				
ルール 例外	DNS シグネチャ			
■ ルール名	重大度		アクション	パケット キャプチャ
b)				
●追加 ■削除 €)上へ 〇下へ 🌀 コピー	🔍 一致するシグネチャを検	出	
				DK キャンセル

(3) 重大度の高いものはパケットキャプチャを実施することにします。
 a)名前に「AS-Rule01(任意)」と入力し、b)パケットキャプチャは「extended-capture」、c)重大度は「critical」と「high」
 にチェックを入れます。d)「OK」をクリックします。

アンチスパイ	(ウェア ルール	0
ルール名	AS-Rule01 a)	
脅威名	any	-
カテゴリ	シウネチャ名の一部として入力されたテキストを含むすべてのシウネチャの熟古に使 any	<i>™</i>
アクション	デフォルト	-
パケット キャ プチャ	extended-capture b)	-
重大度 any (All se ✓ critical ✓ high I ow I ow	everities) C) onal	
	d) ок # +>>t	2N

 (4) 重大度の低いものはパケットキャプチャを実施しないことにします。
 再度、「追加」をクリックし、a)名前に「AS-Rule02(任意)」と入力し、b)パケットキャプチャは「disable」、c)重大度は 「medium」と「low」と「Informational」にチェックを入れます。d)「OK」をクリックします。

アンチスパイ	イウェア ルール	0
ルール名	AS-Rule02 a)	
脅威名	any	
カテゴリ	シグネチャ名の一部として入力されたテキストを含むすべてのシグネチャの燃合に使用 any	-
アクション	デフォルト	-
パケット キャ	disable b)	~
重大度 any (All se critical high ✓ medium ✓ low ✓ informatio	everities) C) onal	
	d) ок <i>+</i> +>>t	π.

(5) a)「DNS シグネチャ」タブをクリックします。
 b)が「sinkhole」となっていること及びシンクホール IPv4 が「72.5.65.111」に設定されていることを確認します。
 (IP アドレスは変更可能です。違うアドレスに変更したいときは、c)をクリックして上書きしてください。)
 d)「OK」をクリックします。

アンチスパイウェア プロファイル		0 🗆
名前 AS-profile01		
内容		
ルール 例外 DNS シグネチャ a)		
■ 外部ダイナミックリストドメイン DNS クエリに対するアクション		0 個の項目s 🗙
Palo Alto Networks DNS 署名 sinkhole b)	■ DNS 脅威 ID 例外 脅威名	
シンクホール IPv4 Palo Alto Networks Sinkhole IP(パロ アルト ネットワーク シンクホールIP) (72.5.65.11	11) v C)	
シンクホール IPv6 IPv6 Loopback IP (::1)	*	
パケット キャプ disable	▼ DNS 脅威 ID	
77		
		d) OK キャンセル

(6) アドレスオブジェクトを登録しておくと、トラフィックログを見たときに Sinkhole による通信が発生したことが判別しやす くなりますので、登録しておきます。

a)「Objects」 \rightarrow b)「アドレス」 \rightarrow c)「追加」をクリックします。

paloalto	Dashboard AC	C Monitor Policies	s Objects Network	Device	🏝 コミット 🧉 🖓 Config 🗸 🔍 検索
			<u>a)</u>		S @^ルプ
אדע b)	N				0個の項目s 🔿 🗙
□ ファトレス グルーフ	名前	場所	タイプ	アドレス	9 <i>1</i> /
 □ アプリケーション □ アプリケーション グループ □ アプリケーション フィルタ 					
※サービス №サービスグループ ◎ タグ	c)				
	🕂 追加 🖃 削除 💿 コピー				

(7) a)名前に「Sinkhole」、b)タイプは「IP ネットマスク」が選択された状態で「72.5.65.111」と入力します。
 c)「OK」をクリックします。

アドレス					0
名前	Sinkhole		a)		
内容					
タイプ	IP ネットマスク	~	72.5.65.111	b)	解決
			スラッシュ表記を使用し ワークを入力します(例 192.168.80.0/24). IPv6 使用したIPv6アドレス(は 2001:db8:123:1::/64	Jて IP アドレスまた !: 192.168.80.150 ま アドレスまたはプレ 例: Ex. 2001:db8:1)も入力できます。	:はネット !たは フィックスを 23:1::1 また
タヴ					•
			c)	OK +	ャンセル

(8) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、c)プロファイル列にあるアイコン をクリックします。

paloalto	1	Dashboard ACC		Monitor	Policie	es Ob	ojects	Network Dev	ice				🍐 コミッ	ト 🗳 🎯 Config	- ♀ 検索
															こ ③ヘルプ
■ セキュリティ b)	٩													9 個0)項目s 🔿 🗙
SY NAT															
日本 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	🛄 dns	💥 application-default	🔮 許可	80 B B	none
 トンネル検査 アプリケーション オーバーライド 	2	NTP	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	🗐 ntp	🔆 application-default	📀 許可	80 G 🔒	
参認証 ↓ DoS プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	🕑 許可	80Ca	8
	4	Youtube	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	j youtube	🔆 application-default	◎ 拒否	none	B
	5	google-drive-web	none	universal	(20) Trust	any	any	any	🕅 Untrust	any	google-drive-web	💥 application-default	😊 許可	80 C 🔒	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	(22) Untrust	any	Risk5_file-sharing	💥 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	没 http 没 service-https	🕑 許可	sogrc)	
	8	intrazone-default 🥹	none	intrazone	any	any	any	any	(intrazone)	any	any	any	O 許可	none	none
	9	interzone-default 🧐	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(9) a)「アンチスパイウェア」で、a)「AS-Profile01」を選択し、b)「OK」をクリックします。

プロファイル		0						
プロファイル タ	イプ プロファイル	-						
アンチウイルス	AV-Profile01	~						
脆弱性防御	VP-Profile01	~						
アンチスパイウェア	AS-Profile01 a)	-						
URL フィルタリング	None							
ファイル ブロッキ ング	FB-Profile01	•						
データ フィルタリ ング	None	•						
WildFire 分析	WF-Profile01	-						
	b) <u> </u>	14						

(10) アクション列が「許可」となっているポリシー全てに、同様の方法でアンチスパイウェアプロファイルを割り当てます。

paloalto		Dashboard ACC		Monitor	Policie	os Ot	ojects	Network Dev	ice				🏄 コミッ	ト 💣 🖓 Config	▼ 9.検索
															ら ③ヘルプ
📟 セキュリティ	9	<u>.</u>												9 個の	0項目s 🚽 🗙
Shat							送信元			洗					
曝 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔟 dns	👷 application-default	📀 許可	SJJ BR	none
	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	mtp	👷 application-default	🔮 許可		B
 ● 認証 ● DoS プロテクション 	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	🔆 application-default	💙 許可	sjoge	
	4	Youtube	none	universal	(22) Trust	any	any	any	122 Untrust	any	youtube	👷 application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🙀 Untrust	any	google-drive-web	👷 application-default	🙁 許可	800 .	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	💥 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	(22) Untrust	any	any	🔆 http 🎉 service-https	💙 許可	87JJA	
	8	intrazone-default 🚳	none	intrazone	any	any	any	any	(intrazone)	апу	any	any	🕑 許可	none	none
	9	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(11)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

12.5.2. 動作確認

アンチスパイウェアの一つの機能である、DNS シンクホールの動作を確認します。

(1) リリースノートから、DNS シグネチャに存在するドメインを確認します。

a)「Device」 → b)「ダイナミック更新」 → c)「現在インストール済み」にチェックが入ったアンチウイルスシグネチャの「リリースノート」をクリックします。

paloalto	Dashboa	rd ACC	Monitor	Policies	Objects	Network	Device		÷	コミット 💣	闷 Config ▾ 鸟 検索
							a)				S @~/l
Netflow	۹.										22 個の項目s 🔿
RADIUS	パージョン	ファイル名		機能	タイ	プ サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント
LDAP	▽ アンチウイル	ス 最終チェッ	• 7: 2018/02/07	23:01:00 JST	スケジュール: Eve	ry hour (Downle	oad and Install)				
Kerberos	2514-3010	panup-all-antivirus-	2514-3010		Full	84 MB	2018/02/07 21:04:56 JST			ダウンロード	リリースノート
ia SAML アイデンティティ フ	2513-3009	panup-all-antivirus-	2513-3009		Full	84 MB	2018/02/06 21:01:42 JST	~	~		リリースノート ()
マルチ ファクター認証 マーカル ユーザー データベー	2511-3005	panup-all-antivirus-	2511-3005		Full	85 MB	2018/02/03 21:04:44 JST			ダウンロード	99-X7-F
2	2512-3007	panup-all-antivirus-	2512-3007		Full	84 MB	2018/02/05 11:29:38 JST	✔ 以前		戻す	リリース ノート
🕵 ユーザー グループ	▼ アプリケーシ	ョンおよび脅威	最終チェック	: 2018/02/08 00:4	i8:47 JST スケジ	ュール: Every h	our at 0 minutes past th	e hour (Download an	d Install)		
IIII スケジュール設定されたログ(777-4484	panupv2-all-content	s-777-4484	Apps, Threats	Full	44 MB	2018/02/07 14:20:15 JST	~	v		リリース ノート [
	770-4445	panupv2-all-content	s-770-4445	Apps, Threats	Full	36 MB	2018/01/24 13:50:00 JST			ダウンロード	リリース ノート
ダイナミック更新 b)	771-4450	panupv2-all-content	s-771-4450	Apps, Threats	Full	36 MB	2018/01/27 03:56:17 JST			ダウンロード	リリース ノート
S7122X	775-4476	panupv2-all-content	s-775-4476	Apps, Threats	Full	36 MB	2018/02/06 08:44:22 JST			ダウンロード	リリース ノート
<i>ᢓ</i> ⋗ サポート	773-4465	panupv2-all-content	s-773-4465	Apps, Threats	Full	36 MB	2018/02/02 14:13:44 JST			ダウンロード	リリース ノート
🔒 マスター キーおよび診断	772 4464	and a state of the state of	- 772 4464	Acces Thursday	P.0	20 10	2010/02/01 07.55.25 307			HAND P	0.0 7 7 8
	ら 今すぐチェッ	ック 📥 アップロー	ド 📘 ファイル	からインストー	6						

(2) リリースノート内の「New Spyware DNS C2 Signatures」でリストされているドメインのどれか一つをコピーします。

(本ガイドでは、「panditgopalsharma.com」を選びました。)

New Spyware DNS C2 Signatures (2085)

generic panditgopalsharma.com
Worm.dorkbot:a.najwahaifamelema48.com
*
Worm dorkhot:a.naiwahaifamelema43.com
Normal on Boctama, Manananan en
consticution and the set
generic.manavimic.com
generic:mzykov.ru
generic:manga247 net
genericinangaz minec

(3) クライアント PC でコマンドプロンプトを開き、a) nslookup を実行します。
 b)選択した「panditgopalsharma.com」のアドレス解決を行います。
 c)Sinkhole の IPv4 アドレス:「72.5.65.111」の返答があることを確認します。

Command Prompt - nslookup	
C:¥Users¥user]>	<u>^</u>
C:¥Users¥userI>	
U;#Users#userI> C:VU=V1>	
C: FUSersFuser12	
C: +Users+user1>	
C:¥llsers¥user1>	
C:¥Users¥user1)nslookup a)	
DNS request timed out.	
timeout was 2 seconds.	
Default Server: UnKnown	
Address: 192.168.45.65	
banditennalsharma.com	
Server: Unknown	
Address: 192.168.45.65	
Non-authoritative answer:	
Name: panditgopalsharma.com	
Addresses: ::]	
72.5.65.111 C)	=
	Ŧ

(4) a)「Monitor」 \rightarrow b)「脅威」で、タイプが「spyware」のログが出力されます。 先頭の「アイコンをクリックして、詳細ログを確認します。

paloalto	Das	shboard	ACC	Monitor	Policies	Objects	Network	Device					きコミッ	/ - 🙆 🎼 Co	infig 🕶 🔍 🕴	検索
													-	手動	S 0	ヘルプ
▼ 🔁 ログ	۹.													• (8 🕀 🎼	🎘 🖗
Bing b)		受信日時	タイプ	名前			送信元ゾーン	宛先ゾーン	送信元アドレス	送信元ユーザー	宛先アドレス	宛先ポート	アプリケーション	アクション	重大度	ファイル
Q URL フィルタリング	P C	04/01 12:18:24	4 spyware	Suspicious Spy.noon:v	DNS Query (Troj www.wanquange.	an- ink)	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	sinkhole	medium	
	Concession of the local division of the loca		*******													

(5) a)送信元の IP が内部 DNS である Windows Server の IP アドレス: 192.168.45.65 であり、b)宛先は上位 DNS の 192.168.55.2 であることは分かります。

しかし、どのクライアントが発した DNS クエリなのかは、この脅威ログからでは判断がつきません。

詳細	コグビュー												0	
全	ار				送信元	Ē				宛先				
: 71	セッション ID アクション アプリケーション ルール 仮想システム パイスのシリアル 番号 IP プロトコル	3137 sinkhole dns DNS udp			送イン	信元ユーザー 送信元 団 ポート ゾーン ターフェイス NAT IP NAT ポート	192.168.45.65 192.168.0.0-19 64330 Trust ethernet1/2 192.168.55.20 20322	a) 2.168.255.1	255	宛先ユ オ インターフコ N NAT オ	-ザー 宛先 192.16 国 192.16 ポート 53 プーン Untrus こイス etherm IAT IP 192.16 ポート 53	8.55.2 8.0.0-192.16 t et1/1 88.55.2	8.255.255	
	ロットリッション 生成日時 受信日時 トンネル タイプ	2018/04/01 2018/04/01 N/A	1 12:18:24 1 12:18:24		詳細	脅威タイプ	spyware Suspicious DNS	Query /Tr	vian-					
					עב	脅威名 ID カテゴリ テンツのバー	197837451 (Vie dns	ew in Threa	e.ink) t Vault)	フラグ	* * -			
						ジョン 重大度 繰り返し回数 ファイル名	medium 2	6-3062		プロキシ トラ クジ パケット ウ	タル ランザ ション 夏号化			
						URL PCAP ID 送信元 UUID 宛先 UUID	0			クライアント サーバーからう	マチャ チャ ーバライ マント			
					電子> 送信	くール へッう 者のアドレス サブジェクト	1			トンネル検護	経済み			
РСАР	受信日時 🔺	_	タイプ	アプリケ	ーション	アクション	ルール	パイト	重大度	カテゴリ	判定	URL	ファイル名	
	2018/04/01 12:1	8:24	spyware	dns		sinkhole	DNS		medium	any				
													ទ បស្រ	

(6) 今度はクライアント PC から、そのドメインに Ping します。

(DNS による IP アドレス解決がなされた後は、一般的に HTTP による通信が多いと思いますが、ここでは簡易的に Ping にしています。 宛先は存在しておらず、Ping も許可していないので、返答はありません。)

🚾 Command Prompt - ping panditgopalsharma.com -t	
C:¥Users¥user1>	^
C:¥Users¥user]>	
C:¥Users¥userlyping panditgopalsharma.com -t	=
Pinging panditgopalsharma.com [72.5.65.111] with 32 bytes of data:	
Request timed out.	

(7) a)「Monitor」→ b)「トラフィック」→ c)「ホストの解決」にチェックを入れると、名前解決が行われます。 このことで、ログの宛先が IP アドレスから「Sinkhole」に変わるので、区別しやすくなります。

先頭の『シアイコンをクリックして、詳細ログを確認します。

paloalto															
NETWORKS	1	Dashboard /	ACC	Monitor	Policies	Objects	Network	Device					81	ミット 🧉 🖓 Config	」▼ ♀ 検索
														手動 🖤	ら ③ヘルプ
V Carr														B X (e 😭 🗃 🕀
場トラフィック D)		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	IPプロトコル	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由	NYA
🐻 URL フィルタリング	Þ	03/17 19:26:32	drop	Trust	Untrust	192.168.45.32		Sinkhole	icmp	0	ping	deny	interzone-default	policy-deny	148
NidFireへの送信	Þ	03/17 19:26:22	drop	Trust	Untrust	192.168.45.32		Sinkhole	icmp	0	ping	deny	interzone-default	policy-deny	148
T F F F F F F F F F F F F F F F F F F F	P	03/17 19:26:17	end	Trust	Untrust	192.168.45.11		199.167.52.141	tcp	443	paloalto-updates	allow	allow outbound web	tcp-fin	12.8k
コーザー ID	Ð	03/17 19:26:11	drop	Trust	Untrust	192.168.45.32		Sinkhole	icmp	0	ping	deny	interzone-default	policy-deny	148
🏠 トンネル検査	P	03/17 19:26:03	end	Trust	Untrust	192.168.45.11		ec2-54-248-11	tcp	443	paloalto-wildfire-cloud	allow	allow outbound web	tcp-rst-from-server	13.3k
 ・ ・ ・				c)				1.compute.am							
	44.4	12345678910	1 🕨	・ 🗹 ホスト名	の解決 📃 ポ	リシーアクショ	ンの強闘表示						ログの表示1-2	0 20 👻 行/1ペー	ジ DESC 👻

(8) a)送信元 IP アドレスが、クライアント PC のアドレスになり、宛先は Sinkhole の IP アドレスです。

この情報が、「192.168.45.32 のクライアント PC は、マルウェア感染の疑いがある」という判断材料になります。

詳細	コグビュー												0 🗖
全般	ł				送信元	t				宛先			
7: : :	セッション ID アクション フションの送信元 アプリケーション ルール ッション終了理由	0 deny from-p ping interze policy	policy pne-default -deny		1	ユーザー アドレス 雌 ポート ゾーン ンターフェイス	- (192.168.4 192.168.0 0 7 Trust (ethernet1	15.32 a 1.0-192.16) 58.255	129-5	2-ザ- マドレス ゴート ゾーン フェイス	72.5.65.111 United States 0 Untrust	b)
デ	カテゴリ 仮想システム パイスのシリアル 番号 IP プロトコル	any icmp			詳細					フラグ キャプティ	ブ ポー タル		-
	ログ アクション 生成日時 開始時間 受信日時 経過時間(約)	2018/ 2018/ 2018/	03/17 19:26:33 03/17 19:26:20 03/17 19:26:33	2 5 2	3	タイフ バイト 受信済みバイト 送信済みバイト	⁷ drop - 148 - 0 - 148			プロキシ パケット	ラションザン 復号ヤチ か		
	を見ている (セントンネル タイプ	N/A			受f 送f	練り返し回劇 パケット 言したパケット 言したパケット 送信元 UUII	2 2 0 2 2			サーバーから 対称! ミラーリン	ナーバー クライ アント リターン ッグ済み		
						宛先 UUII				トンネル村 MPTCP オフ 除外され	き査済み プション れた偵察		
РСАР	受信日時 🔺		タイプ	アプリ ション		アクション		パイト	重大度	カテゴリ	判定	URL	ファイル名
	2018/03/17 19:3	84:51	drop	ping		deny	interzone- default	148		any			0
	2018/03/17 19:3	84:41	drop	ping		deny	interzone- default	148		any			
	2018/03/17 19:3	84:31	drop	ping		deny	interzone- default	74		any			
	2018/03/17 19:3	84:21	drop	pina		denv	interzone-	148		anv			
													閉じる

12.6. URL フィルタリング

URL フィルタリング機能によって、カテゴリ単位に HTTP/HTTPS のアクセス先を制御できます。

パロアルトネットワークス社が、マルウェア、フィッシング、コマンド・アンド・コントロールのような有害な URL をカテゴリとしてまとめたデータベースを5分毎に配信しますので、それらへの通信を容易にブロックすることが可能となります。

それら以外にも、60以上のカテゴリを提供していますので、業務中に参照することは好ましくない URL カテゴリへの通信 はブロックする、ということも可能です。

本ガイドでは、以下の制御を行うことにします。

- ① Malware / Phishing / Command and Control カテゴリ及び有害と考えられる URL カテゴリはブロック。
- ② (一般的に)業務中の参照は好ましくない URL カテゴリは、警告と共に Continue ボタンを出す。
- ③ 識別困難なもの / 識別がなされなかったものについてはアラートのみ。

12.6.1. 設定

(1) a)「Objects」 \rightarrow b)「URL フィルタリング」 \rightarrow c)「追加」をクリックします。

		1010100	Objects	Network Device			🏝 コミット 🧉 🖓 Config 🗝 🔍 検索
							ら @ヘルプ
▼ 🛛 セキュリティ プロファイル 🔍							1 個の項目
 マンチウイルス アンチスパイウェア 名前 	I Contraction of the second	場所	プロック リスト	プロック リストのアクション	許可リスト	サイト アクセス	ユーザー証明書送信
	uit	事前定義済み		block		Allow Categories (57) Alert Categories (0) Continue Categories (0) Block Categories (9) Override Categories (0)	Allow Categories (65) Alert Categories (0) Continue Categories (0) Block Categories (0)

(2) 名前に「UF-Profile01(任意)」と入力します。

URL フィルタリング プロファ・	イル			0
名前	UF-Profile01			
内容				
カテゴリ オーバーライド	URL フィルタリング設定	ユーザー証明書検出		
	1	-		
				66 個の項目s → 🗙
🔲 カテゴリ			サイト アクセス	ユーザー証明書送 信
abortion			allow	allow
abused-drugs			allow	allow
adult			allow	allow

(3) アクションを「Block」に設定するカテゴリは、以下とします(アルファベット順)。

URL カテゴリ名		カテゴリ説明
Abused Drugs	(乱用薬物)	合法および非合法を問わず薬の乱用を促進するサイト、薬物関連の道具の使 用や販売、薬の製造や販売に関連するサイト。
Command and Control	(コマンドとコントロール)	マルウェアまたは侵害されたシステムが使うURLやドメイン。 それらの感染システムが、不正コマンドを受信するためや、データを送信するこ とを目的として、攻撃者のリモートサーバーへ密かに通信する際に利用する宛 先。
Copyright infringement	(著作権侵害)	著作権を侵害したビデオや映画、その他のメディアファイルをダウンロードにより提供する専用のウェブサイトやサービス。
Dynamic DNS	(ダイナミック DNS)	提供されたまたは動的なドメイン名と IP アドレスを関連付けるためにダイナミック DNS サービスを利用しているサイト。ダイナミック DNS サイトは、サイバー 攻撃者に対する C&C 通信および、他の悪意のある目的のために使用される 場合がある。
Extremism	(過激主義・思想)	テロや人種差別、ファシズムや人種、異なる民族的背景、宗教や信仰を判別する過激主義・思想を促進するウェブサイト。
Malware	(マルウェア)	悪意あるコンテンツ、実行可能ファイル、スクリプト、ウイルス、トロイの木馬、コ ードを含むサイト。
Parked	(パークドメイン)	限られたコンテンツやクリックスルー広告をホストする URL。ホストに対して収入を生むことがあるが、一般にはエンドユーザにとって有用なコンテンツやサイトが含まれていない。工事中のサイトやフォルダのみのページを含む。
Peer-to-Peer	(ピアツーピア)	ターゲットファイルへのデータ、ダウンロードしたプログラム、メディアファイル、 その他ソフトウェアアプリケーションへのピアツーピア共有アクセスまたはクライ アントを提供するサイト。シェアウェアやフリーウェアサイトは含まない。 bittorrent ダウンロード機能を持つサイトが主に含まれる。
Phishing	(フィッシング)	フィッシングやファーミングによりユーザーから個人情報を取得する、見かけ上は信頼できそうなサイト。
Proxy Avoidance and Anonymizers	(プロキシ回避と 匿名プロキシ)	プロキシサーバーやその他方式で URL フィルタリングや URL 監視をバイパス するサイト。
Questionable	(疑わしいサイト)	下品なユーモア、特定層の個人やグループをターゲットにした不快なコンテン ツ、犯罪行為、違法行為、手早く金持ちになれる、といったものを含むサイト。

a)上記のリストに記載されたカテゴリの先頭にチェックを入れます。

b)「サイトアクセス」右横の▽をクリックして表示された中から、c)「選択したアクションの設定」 → d)「block」を選択します。 e)「OK」をクリックします。

U	RLフ	ィルタリング プロファー	(JL			0	
		名前	UF-Profile01				
		内容					
C							
	カテ	ゴリオーバーライド	URL フィルタリング設定	ユーザー証明書検出			
						b) 16 個の項目s → 🗙	
		カテゴリ			サイト アクセ	ユーザー証明書送 信	
a		online-storage-and-backup			allow	2↓ 昇順	
		parked			allow	2↓ 隆順	
	V	peer-to-peer			allow		
		personal-sites-and-blogs			allow	カラム I	> _
		philosophy-and-political-advocad	γ.		allow		
		phishing			allow	すべてのアクションの設定	
		private-ip-addresses			allow	C) 選択したアクションの設定	allow
		proxy-avoidance-and-anonymize	rs		allow	THE STREET	alert
		questionable			allow	タリの目的型	d)
H		real-estate			allow	allow	DIOCK C)
	8 hex	digits: 00000000 to FFFFFFFF					continue
	URL	. カナコリをナェック					override
							none
						OK キャンセル	

(4) アクションを「Continue」に設定するカテゴリは、以下とします(アルファベット順)。

URL カテゴリ名		カテゴリ説明 オート・シート アイ・シート アイ・シート アイ・シート アイ・シート アイ・シート
Adult	(アダルト)	性的に露骨な内容、文章(言葉を含む)、芸術、または本質的に性的表現がきわどい製品、オンライングループやフォーラム。ビデオチャット、エスコートサービス、ストリップクラブを含むアダルトサービスを宣伝するサイト。ゲームやコミックであれアダルトコンテンツを含むものはすべて adult にカテゴリ化される。
Dating	(出会い系)	出会い系、オンラインデートサービス、アドバイス、その他個人的な広告を提供するウェブサイト。
Gambling	(ギャンブル)	本物または仮想のお金の交換を容易にする宝くじやギャンブルの Web サイト。賭けのオッズ やプールに関する情報、ギャンブルに関する指導や助言を提供するサイト。ギャンブルを行わ ないホテルやカジノの企業サイトは Travel にカテゴリ化される。
Games	(ゲーム)	ビデオやコンピュータゲームをオンライン再生やダウンロードできるサイト、ゲーム批評、ヒント、裏技を提供するサイト。非電子ゲームの教育、ボードゲームの販売や交換、関連する出版物やメディアに関するサイト。オンライン懸賞や景品を扱うサイトを含む。
Hacking	(ハッキング)	通信機器やソフトウェアに対して、違法または疑わしいアクセスや利用に関するサイト。ネット ワークやシステムが侵害される可能性のあるプログラムの開発や配布、手順の助言やヒント に関するサイト。また、ライセンスやデジタル著作権システムをバイパスさせるサイトも含まれ る。
Weapons	(武器)	兵器やその使用に関する、販売、批評、説明、取扱のサイト。

UF-Profile01をクリックして、もう一度プロファイル設定画面を開きます。

a)上記のリストに記載されたカテゴリの先頭にチェックを入れます。

b)「サイトアクセス」右横の▽をクリックして表示された中から、c)「選択したアクションの設定」 → d)「Continue」を選択しま す。e)「OK」をクリックします。

URL フィルタリング プロファ・	rル		0	
名前	UF-Profile01			
内容				
カテゴリオーバーライド	URL フィルタリング設定 ユーザー証明書検出			
•		b) ⁶ 個	の項目s 🔿 🗙	
■ カテゴリ		サイト アクセ <mark>スマ</mark> 信	ザー証明書送	_
a)		allow 2↓ 昇J	頁	
Training-and-tools		allow Z 译	۵.	
		allow		
Travel		allow	∍⊿ ▷	
		allow す	べてのアクションの設定 ▶	
Veapons		allow	21.たマクションの設定 ▶	
veb-advertisements		allow		allow
veb-based-email		allow 列(の調整	alert
veb-hosting		allow allow	·	block
8 hex digits: 00000000 to FFFFFFF				continue d)
URL カテゴリをチェック				override
				overnae
		е) ок	キャンセル	none

(5) アクションを「Alert」に設定するカテゴリは、以下とします(アルファベット順)。

URL カテゴリ名		カテゴリ説明
Insufficient Content	(識別困難な Web サイト)	テストページやコンテンツが存在しない場合やユーザ向けではない API アクセ ス用のサイト、コンテンツの表示に認証必要などカテゴリ分類が困難な Web サイト。
Not-resolved	(未解決)	Web サイトがローカル URL フィルタリングデータベースに見つからず、ファイ アウォールが、カテゴリをチェックするためにクラウドの URL データベースに接 続を試みたが、接続できなかった状態を示す。
		URL カテゴリの参照が実行されると、PA Firewall は以下の順で検索を行う。 ① データプレーンの URL キャッシュをチェック ② 管理プレーンの URL キャッシュをチェック ③ クラウド内の URL データベースへ問い合わせる。
Unknown	(未知)	Web サイトはまだ分類されていないため、PA Firewall の URL フィルタリング データベースまたは URL クラウドデータベースには存在しないことを示す。

UF-Profile01をクリックして、もう一度プロファイル設定画面を開きます。

a)上記のリストに記載されたカテゴリの先頭にチェックを入れます。

b)「サイトアクセス」右横の▽をクリックして表示された中から、c)「選択したアクションの設定」 → d)「Alert」を選択します。 e)「OK」をクリックします。

URL フィルタリング プロフ	アイル	Ø	
	名前 UF-Profile01		
	内容		
カテゴリ オーバーライ	ド URL フィルタリング設定 ユーザー証明	月書検出	
٩		b) ⁶ 個の項目s → 🗙	
🔲 カテゴリ		サイト アクセ マ ユーザー証明書送	
		21000 2↓ 昇順	
raining-and-tools	parei	allow Z↓降順	
franslation		allow	
Travel		allow	
🔽 unknown		allow すべてのアクションの設定	•
weapons		continue 選択したアクションの設定	A start
veb-advertisements		allow	dilow
veb-based-email		allow 列の調整	alert U)
veb-hosting		allow	block
8 hex digits: 00000000 to FFFFFFFF			continue
URL カテゴリをチェック			override
			none
		e) ок キャンセル	

(6) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、c)プロファイル列にあるアイコン をクリックします。

															S ()~//
■ セキュリティ b)	٩													9個0	D項目s 🍠 🕄
ar NAI							送信元			8 先					
 ペースフォワーディング 2 復号 ▲ トンネル検査 ■ アプリケーションオーパーライト 		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🛄 dns	👷 application-default	♥ 許可	800 6	none
	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	m ntp	👷 application-default	📀 許可		
会認証 ↓ DoS プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	2 application-default	🕑 許可	800GR	
	4	Youtube	none	universal	(22) Trust	any	any	any	(22) Untrust	any	j youtube	👷 application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	google-drive-web	👷 application-default	📀 許可	800 0	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	☆ http ☆ service-https	🕑 許可		
	8	intrazone-default 🧇	none	intrazone	any	any	any	any	(intrazone)	any	any	any	♥ 許可	none	none
	9	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(7) a)「URL フィルタリング」で、a)「UF-Profile01」を選択し、b)「OK」をクリックします。

プロファイル		0
プロファイル う	イプ プロファイル	•
アンチウイルス	AV-Profile01	~
脆弱性防御	VP-Profile01	~
アンチスパイウェア	AS-profile01	-
URL フィルタリング	UF-Profile01 a)	-
ファイル ブロッキ ング	FB-Profile01	•
データ フィルタリ ング	None	•
WildFire 分析	WF-Profile01	•
	b) OK キャンセ	ιL

(8) アクション列が「許可」となっていて、HTTP/HTTPS 通信が発生するポリシーに、同様の方法で URL フィルタリングを 割り当てます。

														2.4	
10 セキュリティ	٩													9個0)項目s 🏓 🗙
NAT		1					送信元			的先				1	
⊕ポリシー ベース フォワーディング		名前	タヴ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
御 復号 ひょうし くうしょう しょう しょう しょう しょう ひょうしょう オーバーライド ひまます ひょう プロテクション ひのち プロテクション	1	DNS	none	universal	(20) Trust	any	any	any	(22) Untrust	any	🔟 dns	🔆 application-default	🕑 許可	8000 da	none
	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔟 ntp	💥 application-default	🕐 許可		
	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	💙 許可	SCOCE.	
	4	Youtube	none	universal	(20) Trust	any	any	any	(22) Untrust	any	j youtube	👷 application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	апу	апу	any	(22) Untrust	any	google-drive-web	💥 application-default	📀 許可		
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	(22) Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	🔆 http 🎉 service-https	🕑 許可	sjoge ^r	
	8	intrazone-default 🔮	none	intrazone	any	any	any	any	(intrazone)	any	any	any	⊘ 許可	none	none
	9	interzone-default 🏼 🎯	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

- (9) デフォルトでは、一度 Continue を実施すると、15 分間は再度アクセスしても Continue 画面がでません。
 動作確認テスト時の15 分は長いので、最短の1 分に一時的に変更します。
 - a)「Device」 \rightarrow b)「セットアップ」 \rightarrow c)「コンテンツ ID」で表示された URL フィルタリングの d) $\stackrel{\odot}{\stackrel{\circ}{\xrightarrow}}$ をクリックします。

m paloalto							_			
NETWORKS®	Dashboard AC	C Monitor	Policies	Objects	Network	Device				
						/	,			
闷 セットアップ b)	管理 操作 サー	ビス インターフ	ェイス テレ	~×トリー	コンテンツЮ	WildFire	セッシ	ョン HSM		
	· · · · · · · · · · · · · · · · · · ·				C)					
	URL フィルタリング			L L			d) 🇱	コンテンツ) 設定	
タイスウート フロファイル 9 管理者	<i>\$</i> 1	ナミック URL キャッショ	ュのタイムアウト	(時間) 168			<u>u)</u>		復号化されたコン	テンツの転
😥 管理者ロール		URL コンティニ			拡張パケット キャプ	チャ長 (パ・				
総認証プロファイル		IIPI 管理オーバーラ			TCP Ano-ID絵査キューを報過	+++1/1				
2015年1月11日 2015年1月110年1月111日 2015年1月110年1月111日 2015年1月110年1月111日 2015年1月110年1月110年1月1110年1月1110年1月1110年1月1110年1月110年1月1110年1月1110年1月1110年1月1110年1月1110年1月1110年1月1110年1月1110年1月110年1月110年1月110年1月110年1月11111111				(/) 20						
■▲ ユーザー ID		URL 管理ロックア	9191979	r (22) 30					TCPコンテンツ検査キューを超過し	たセグメン
型VM 情報ソース			PAN-DB サ	-/(-					UDPコンテンツ検査キューを超過した	データグラ
▽し言証明書の管理									HTTPヘッダーレン	/ジオプショ
							_			
ここのCSP レフポンダ	URL 管理オーバーライ	۴							And	
	APF SS	/TLS サービス プロファ	イル モー		プロパティ			A-FUI Warueu-FU	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	
							_		User-ID ੱੋ X-Forward	ied-For ヘッ
🔒 SSL 復号化例外									X-Forward	Jed-For ヘッ
◎応答ページ										
🔁 ログ設定									100 AIS	
▽ 👘 サーバー プロファイル	4								微胞	
							-	□◎ ≓_万厚端の	0.005.1383	

(10) a)URL コンティニュータイムアウト(分)を「1」に変更して、b)「OK」をクリックします。



(11)「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

12.6.2. 動作確認

(1) クライアント PC の Web ブラウザで、パイレート・ベイ (http://thepiratebay.org) ヘアクセスします。

このサイトは、スウェーデンのインデックスサイト(Torrent ファイルを検索するサイト)であり、Peer-to-Peer のカテゴリに属しています。

以下のように、ブロックされたことを示す画面が表示されます。

A C 2	3
\leftarrow \rightarrow C $\textcircled{0}$ thepiratebay.org	:
Web Page Blocked	
Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.	
User: acme\user1	
URL: thepiratebay.org/	
Category: peer-to-peer	

(2) クライアント PC の Web ブラウザで、IGN Entertainment (<u>http://www.ign.com</u>) ヘアクセスします。

このサイトは、ビデオゲームを中心としたいくつかの娯楽に関する報道を行うWebサイトであり、Gamesカテゴリに属しています。

以下のように、ブロックされたことの警告と共に、「Continue」ボタンを表示します。



「Continue」をクリックすることで、本サイトが表示されることを確認してください。

(3) a)「Monitor」→ b)「URL フィルタリング」で、URL のフルパスを含んだログが確認できます。 先頭の「アイコンをクリックして、詳細ログを確認します。

		Dashboard	ACC	Monitor Polici	es Objects Network	Device				\$	コミット 省 阔	Config - 9、検索
				a)							手動	S @∿/
▼ 🔂 ログ	•										9	x 🕀 📪 🎥
キャトラフィック の みの		受信日時	カテゴリ	URL		送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	アプリケーション	アクション
url フィルタリング b)	P	03/18 12:23:33	games	apps.ign.com/video-player,	/fonts/v61-player-icons.woff	Trust	Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
Witchire NOTZIE	P	03/18 12:23:33	games	apps.ign.com/video-player,	/fonts/ffdin700normal.woff	Trust	Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
■ データ フィルタリング ■ HIP マッチ	P	03/18 12:23:33	games	apps.ign.com/video-player,	/fonts/ars400normal.woff	Trust	Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
I ユーザー ID	D 03/18 12:23:33 games				/fonts/ars900normal.woff	Trust	Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
🚵 トンネル検査	P	03/18 12:23:33	8 12:23:33 games apps.ign.com/video-player/fonts/ars700normal.woff				Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
₩ 設定 ■ システム	P	03/18 12:23:33	games	comments.ign.com/api/v1/	ign/assets/count	Trust	Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
	P	03/18 12:23:33	games	g.ign.com/ign.js?cc=JP&cc	p=geocc=JP&url=http://www.ign.com	/ Trust	Untrust	192.168.45.32		104.113.96.23	web-browsing	continue
I BEE	P	03/18 12:23:32	games	zdstatic.ign.com/js/zddmp/	1.1/zddmp.min.js	Trust	Untrust	192.168.45.32		104.78.220.98	web-browsing	continue
■ 統合済み ● パケット キャプチャ	P	03/18 12:23:32	games	apps.ign.com/video-player,	/release/6.2.4/default.becf9b30.js	Trust	Untrust	192.168.45.32		151.101.73.135	web-browsing	continue
▼ 🖓 アプリケーション スコープ	D	03/18 12:23:31	games	www.ign.com/		Trust	Untrust	192.168.45.32		184.26.223.73	web-browsing	continue
🔛 サマリー	図 サマリー D 03/18 12:23:29 games www.ign.com/					Trust	Untrust	192.168.45.32		184.26.223.73	web-browsing	block-continue
◎ 変化モニター	P	03/18 12:23:26	peer-to-peer	thepiratebay.org/favicon.ic	0	Trust	Untrust	192.168.45.32		104.27.216.28	web-browsing	block-url
	P	03/18 12:23:26	peer-to-peer	thepiratebay.org/		Trust	Untrust	192.168.45.32		104.27.216.28	web-browsing	block-url

(4) 詳細ログです。

もし、この URL がこのカテゴリに属していることが間違っていると思われる場合には、以下の「詳細」内にある「分類の 変更要求」をクリックすることで、パロアルトネットワークス社に変更要求を送ることができます。

詳細口	コグビュー													0 🗖
全般	ł				送信元	ī.				宛先				
ד דיו	セッション ID アクション アプリケーション ルール 仮想システム ペイスのシリアル 番号 IP プロトコン	23259 block-co web-bro allow ou tcp	ontinue owsing utbound web		73	ユーザー アドレス 国 ポート ゾーン ンターフェイス NAT IP NAT ポート	192.168.45.3 192.168.0.0 50533 Trust ethernet1/2 192.168.55.2 14351	32 192.168.2! 20	55.255	ユ ア インターフ NAT	ーザー ドレス 国 ト ン エイトン ANAT IP ポート	184.26.2 United St 80 Untrust ethernet: 184.26.2 80	23.73 rates 1/1 23.73	
нтте	カテゴリ 生成日時 受信日時 トンネルタイプ	games 2018/03 2018/03 N/A	3/18 12:23:29 3/18 12:23:29		詳細	重大度 繰り返し回数	informationa 1	1	_	フラグ キャプティ: プロキシトク パケット	ブ ラシ 復 キ ール ザン 化 プャ			
	ーザー エージェ ント Referrer X-Forwarded-For					HTTP 方式	分類の変更到 get	臣求		クライアン サ サーバーから トンネル検 証明書が検出	トー クア 査 さ しん また			
PCAP	受信日時 🔺		タイプ	アプリケ ン	ーショ	アクション	ルール	バイト	重大度	カテゴリ	判定	u	IRL	ファイル名
	2018/03/18 12:2	23:44	end	web-bro	wsing	allow	allow outbound web	1092		games				
	2018/03/18 12:2	23:29	url	web-bro	wsing	block- continue	allow outbound web		informationa	l games		V	/ww.ign.c	
														閉じる

(5) 表示された画面のフォームを埋めて、「送信」をクリックしてください。 (※このステップは、「間違っている」と思われる場合だけ実施し、テストとしての実施は控えてください。)



12.7.データフィルタリング

データ フィルタリングを使用すると、PA Firewall はクレジットカード番号等の機密情報を検出し、このようなデータが漏洩 することを防ぐことができます。

本ガイドでは、クレジットカード番号の漏洩を防ぐことを目的とした設定を行います。

- ① Web サイトに対して、クレジットカード番号を1つ送信することは許容します。
- ② Web サイトに対して、クレジットカード番号を2つ送信する場合はアラートを出力します。
- ③ Web サイトに対して、クレジットカード番号を3つ以上送信する場合はブロックします。

12.7.1. 設定

(1) a)「Objects」 \rightarrow カスタムオブジェクトの下の b)「データ パターン」 \rightarrow c)「追加」をクリックします。

paloalto	Dashboard ACC	Monitor Policies Object	cts Network Device		2	コミット 者 陽 Config - 🔍 検索
						😋 🔞 ヘルプ
🖻 🕵 GlobalProtect						0個の項目s 🔿 🗙
● 外部ダイナミック リスト	プロファイル		パターン			
🗓 データ パターン b)	名前	場所	タイプ	名前	デフォルト ファイル タイプ	パターン
	c)					

(2) a)名前に「CC Number(任意)」と入力し、b)パターンタイプで「事前定義済みのパターン」を選択します。
 c)「追加」をクリックして、d)「クレジットカード番号」を選択します。e)「OK」をクリックします。

データ パターン			0
名前 CC Number	a)		
内容			
パターン タイプ 事前定義済み	・のパターン b)		•
۹.		1 個の項目 🔿	×
□ 名前	内容	ファイル タイプ	
クレジット カード番号 d)	米国のクレジット カード番号のパター ン	- いずれか	
c)			
母 追加 ■ 削除			
		<mark>е)</mark> ок + +>+	ν

(3) a)「Objects」 → セキュリティプロファイルの下の b)「データフィルタリング」 → c)「追加」をクリックします。

paloalto	Dashboard	ACC	Monitor Policies	Objects	Network Device				📥 コミット	🕯 陽 Config 🔻 🔍 検索
										🔓 🔞 ヘルプ
🕢 外部ダイナミック リスト	۹.									0個の項目s 🗙
▶ → → → → → → → → → → → → → → → → → → →	🗖 名前	場所	データ キャプチャ	データ パターン	アプリケーション	ファイル タイプ	方向	アラートしきい値	プロックしきい値	ログ重大度
	C)									

(4) a)名前に「DF-Profile01(任意)」と入力し、b)「追加」をクリックします。
 c)設定済みの「CC Number」を選択、d)「upload」、e)アラートしきい値に「2」、f)ブロックしきい値に「3」と入力します。
 g)「OK」をクリックします。

データフィルタ	リングプロファ・	7 <i>1</i> L				0 🗆
名前	DF-Profile01	a)				
内容						
	ニ データ キャプチャ					
۹.					1 (i	🛙 の項目 🔿 🗙
■ データ パター ン	アプリケーション	ファイル タイプ	方向	アラートしき い値	プロックしき い値	ログ重大度
CC Number	any	いずれか	upload	2	3	informational
			u)	e)	1)	J
b)						
➡追加 ■削除						
アラート/プロックしきい	值: (0-65535)				1	
) ок	キャンセル

(5) a)「Policies」→ b)「セキュリティ」で表示された「allow outbound web」ポリシーの、c)プロファイル列にあるアイコン をクリックします。

paloalto	1	Dashboard ACC		Monitor	Polici	es Ob	ojects	Network Dev	ice				813	:ット 者 陽 Config	- Q.検索
					a)									1	ら のヘルプ
💷 セキュリティ b)	٩				<u> </u>									9 個0	D項目s 📑 🗶
an Indi							送信元			ē先					
日本 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
◎ 復号	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	📰 dns	👷 application-default	📀 許可	SJUER.	none
トンネル検査 アプリケーション オーバーライド	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	📰 ntp	👷 application-default	🔮 許可		
参認証 ↓ DoS プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	💥 application-default	🔮 許可	8000 6 8	
	4	Youtube	none	universal	(22) Trust	any	any	any	(22) Untrust	any	j youtube	💥 application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	google-drive-web	👷 application-default	🔮 許可		B
	6	Risk5_file-sharing	none	universal	(20) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	💥 application-default	◎ 拒否	none	B
	7	allow outbound web	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	any	🔆 http 🎉 service-https	🕑 許可	C	
	8	intrazone-default 🥹	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
	9	interzone-default 🧇	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(6) a)「データフィルタリング」で、a)「DF-Profile01」を選択し、b)「OK」をクリックします。

プロファイル		0
プロファイル う	アイプ プロファイル	•
アンチウイルス	AV-Profile01	•
脆弱性防御	VP-Profile01	•
アンチスパイウェア	AS-Profile01	•
URL フィルタリング	UF-Profile01	•
ファイル ブロッキ	FB-Profile01	•
テーダ フィルタリ ング	DF-Profile01 d)	*
WildFire 分析	WF-Profile01	•
	b) <u>OK</u> ++>+	n

(7) Upload 方向へのクレジットカード番号の漏洩があり得るポリシーへ、同様の方法でデータフィルタリングプロファイル を割り当てます。

paloalto	1	Dashboard ACC		Monitor	Policie	es Ob	jects	Network Dev	ice				≛⊐3	ミット 💣 闷 Config 🕶	Q 検索
														9	のヘルプ
📾 セキュリティ	٩													9 個の項	🗉 🔿 🗙
Start Cos							送信元			统					1
職ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
◎ 復号	1	DNS	none	universal	(22) Trust	any	any	any	(22) Untrust	any	🔝 dns	👷 application-default	🕑 許可	8000	none
ドンネル検査 アプリケーション オーバーライド	2	NTP	none	universal	(22) Trust	any	any	any	(22) Untrust	any	mtp	👷 application-default	📀 許可		
参認証 () DoS プロテクション	3	Youtube-streaming	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	youtube-base	🗶 application-default	🔮 許可		
	4	Youtube	none	universal	(20) Trust	any	any	any	(22) Untrust	any	i youtube	💥 application-default	◎ 拒否	none	
	5	google-drive-web	none	universal	(22) Trust	апу	any	апу	🕅 Untrust	any	google-drive-web	👷 application-default	🕑 許可	SCOCES.	
	6	Risk5_file-sharing	none	universal	(22) Trust	any	any	any	🕅 Untrust	any	Risk5_file-sharing	👷 application-default	◎ 拒否	none	
	7	allow outbound web	none	universal	(22) Trust	any	влу	any	(22) Untrust	any	any	🔆 http 🎉 service-https	🥴 許可	9777784 <u>8</u>	
	8	intrazone-default 🚳	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可	none	none
	9	interzone-default 🚳	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	

(8) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

12.7.2. 動作確認

(1) 下記サイトに記載のあるクレジットカード番号を利用してテストします。

Testing Alerts for Data Filtering https://live.paloaltonetworks.com/t5/Management-Articles/Testing-Alerts-for-Data-Filtering/ta-p/67241

- (2) Dropbox サイト (www.dropbox.com) や Google ドライブサイト (drive.google.com) のような、ファイルの Upload が可能なサイトへアクセスします。(本ガイドでは、Dropbox を利用します。)
- (3) クライアント PC 上で、以下のクレジットカード番号(1個)を持つ txt ファイルを作り、Dropbox へ Upload します。

5376-4698-9386-4886

ファイル名:1CC.txt

(4) クライアント PC 上で、以下のクレジットカード番号(2個)を持つ txt ファイルを作り、Dropbox へ Upload します。

5376-4698-9386-4886 5564-8017-1758-1316

ファイル名:2CC.txt

(5) クライアント PC 上で、以下のクレジットカード番号(3 個)を持つ txt ファイルを作り、Dropbox へ Upload します。 (エラーになります。)

5376-4698-9386-4886 5564-8017-1758-1316 5559-4615-4452-4711

ファイル名:3CC.txt

 (6) クライアント PC 上で、以下のクレジットカード番号(10 個)を持つ txt ファイルを作り、Dropbox へ Upload します。 (エラーになります。)

5376-4698-9386-4886 5564-8017-1758-1316 5464-9730-1302-5263 5257-2750-0534-2578 5564-9616-5310-6823 5483-3128-3984-7229 5352-9543-2663-9003 5130-0484-5710-3076 5210-3641-5712-1745 5559-4615-4452-4711

ファイル名:10CC.txt

(7) a)「Monitor」 → b)「データフィルタリング」で、ログを確認します。

paloalto	_	Dashboard	ACC	Monitor	Policies	Obj	ects N	etwork [Device					ふ コミッ	ト 💣 😡 Con
														手	10 V
▼ 📴 ログ	۹,														⇒ ×
N トラフィック		受信日時	カテゴリ		ファイル名	URL	名前	送信元ゾーン	宛先ゾーン	送信者	送信者名	受信者	宛先ポート	アプリケーション	アクション
RURL フィルタリング	P	03/18 13:47:5	1 online-sto	rage-and-backup	10CC.bxt		CC Number	Trust	Untrust	192.168.45.32		162.125.80.6	443	dropbox-uploading	reset-server
MildEiroo. (D)#/E	Þ	03/18 13:47:4	3 online-sto	rage-and-backup	3CC.txt		CC Number	Trust	Untrust	192.168.45.32		162.125.80.6	443	dropbox-uploading	reset-server
□ データ フィルタリング D		03/18 13:47:3	3 online-sto	rage-and-backup	t	4	CC Number	Trust	Untrust	192.168.45.32		162,125,80.6	443	dropbox-uploading	alert

13. User-ID

User-ID を使うことで、ログや ACC やレポートを、IP アドレスではなく、ユーザ名で可視化できるようになります。

加えて、ポリシーの送信元も IP アドレスやサブネットではなく、ユーザ名やユーザグループで設定できるようになります。

User-ID は様々な認証基盤との連携が可能ですが、本ガイドでは、Active Directory(以降、AD)と連携して、ログにユーザ 名を表示させる設定を行います。

AD のログには、「どのユーザーにどの IP アドレスが割り当てられているか」の情報が存在しており、PA Firewall はその 情報を取得して内部でデータベース化します。

PA Firewall にパケットが到達した時点で、パケットの送信元 IP アドレスをチェックし、User-ID データベースと照合して、 その IP アドレスと紐付いたユーザー名をログに表示します。

本ガイドでは、最も簡易的な方法である、WMIを使った「エージェントレス User-ID」という方式の設定を行います。

[WMI (Windows Management Instrumentation)]: Windows を管理するための API こと。

13.1.設定

13.1.1. Windows Server 2012 R2

PA Firewall が AD のログを取得できるようにするための、AD 側の設定例を示します。

この AD に事前に設定されているドメインは「acme.com」です。

(1) AD のログを取得できる権限を持つユーザを AD に追加します。

「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。 a)「acme.com」 → b)「Users」を右クリック → c)「New」 → d)「User」をクリックします。

			Active Dire	ectory Users and	Computers		_ _ ×		
File Action View Help									
⇐ ⇒ 🙇 🖬 🔏 📋 🗙 🗎 🧔) 🗟 🛛	1 🖬 🙁 😣	16 🍸 🗾 🐍						
Active Directory Users and Computers	[Win2012	acme.com]	Name 📩		Туре		Description	~	
b Saved Oueries			گ Administrator		User		Built-in account for administering the computer/domain		
⊿ 🛱 acme.com 🛛 a)			& Allowed RODC Passwo	rd Replication Group	Security Group - Don	omain Local	Members in this group can have their passwords replicated		
D Builtin			용 Cert Publishers		Security Group - Don	omain Local	Members of this group are permitted to publish certificate:		
Computers			& Cloneable Domain Cor	ntrollers	Security Group - Glo	obal	Members of this group that are domain controllers may be		
Domain Controllers			& Denied RODC Password	d Replication Group	Security Group - Don	omain Local	Members in this group cannot have their passwords replica		
ForeignSecurityPrincipals			Section 2 March 2 Marc		Security Group - Don	omain Local	DNS Administrators Group	-	
Hear by			🍇 DnsUpdateProxy	Security Group - Glob	obal	DNS clients who are permitted to perform dynamic update			
Delegate Control			🍇 Domain Admins	Security Group - Glo	obal	Designated administrators of the domain			
Find			& Domain Computers	Security Group - Glo	obal	All workstations and servers joined to the domain			
New	•	Computer	da	1	Security Group - Glo	obal	All domain controllers in the domain		
		Computer			Security Group - Glo	obal	All domain guests		
All Tasks	•	Contact			Security Group - Glo	obal	All domain users		
View	•	Group			Security Group - Univ	niversal	Designated administrators of the enterprise		
Refresh		InetOrgPe	rson	omain Controllers	Security Group - Univ	niversal	Members of this group are Read-Only Domain Controllers		
Export List		msDS-Res	ourcePropertyList	wners	Security Group - Glo	obal	Members in this group can modify group policy for the do		
Export Eist		msImagin	g-PSPs		User		Built-in account for guest access to the computer/domain		
Properties	MSMO Ou	eue Alias		Security Group - Don	omain Local	-	-		
Help		Printer		Ш			>		
Create a new object		User (()						
		Shared Fol	der						

(2) 「panagent@acme.com」というユーザを生成します。

	New Object - User
🧏 Create in	: acme.com/Users
First name:	pan a) Initials:
Last name:	agent b)
Full name:	pan agent
User logon name:	
panagent	C) @acme.com v
User logon name (pr	e-Windows 2000):
ACME¥	panagent
	< Back d) Next > Cancel

(3) a)パスワードを入力し、b)「User must change password ad next login/ユーザは次回ログイン時にパスワードの変 更が必要」のチェックを外します。c)「Next」をクリックします。

New Object - User
Create in: acme.com/Users
Password: a) Confirm password:
User must change password at next logon b)
User cannot change password
Password never expires
Account is disabled

(4) 「Finish」をクリックします。

New Object - User	×
Create in: acme.com/Users	
When you click Finish, the following object will be created:	
Full name: pan agent	^
User logon name: panagent@acme.com	
	~
	C
< Back Finish	Cancel

(5) 生成した「pan agent」をダブルクリックして開き、a)「member of」タブをクリックします。
 b)「Add」をクリックして、c)3 つのグループ:「Distributed COM Users」、「Event Log Readers」、「Server Operators」
 を付与します。d)「OK」をクリックします。

	pan agei	nt Prope	erties	? X						
Remote control	Remote D	Desktop Se	rvices Profile	COM+						
General Address	Address Account Profile Telephones Orga									
Member Of	Member Of Dial-in Environment Sea									
a)		-								
Member of:	A									
Name Distributed COM U	Active Dire	ectory Dom	nain Services Fo	der						
Distributed COM Us	ers acme.com	1/Builtin								
Event Log Readers	acme.com	/Builtin								
Server Operators	acme.com	v/Builtin	c)							
			٥/							
<	-			>						
Add b)	Remove									
Primary group: D	Primary group: Domain Users									
Set Primary Group	There is n you have application	o need to o Macintosh ns.	change Primary clients or POSI)	group unless (-compliant						
Set Primary Group	There is n you have application	o need to (Macintosh ns.	change Primary (clients or POSI)	group unless K-compliant						

(6) Windows PowerShell を開き、「wmimgmt.msc」と入力して Enter キーを押します。



(7) a)「WMI Control」を右クリックして Properties を選択し、b)「Security」タブをクリックします。
 c)「CIMV2」を選択して、d)「Security」をクリックします。

WmiMgmt - [Console Root\WMI Contr	rol (Local)]
🚡 File Action View Favorites Window Help	
Console Root	Actions
WMI Control (Local) a) Windows Management Instrumentation (WMI)	WMI Control (Local)
WMI Control (Local) Properties ? X b General Backup/Restore Security Advanced	More Actions
Namespace navigation allows you to set namespace specific security.	
Root AccessLogging Accestoff AccessLogging AccessLogging AccessLogging Ac	
OK Cancel Apply	

 (8) a)「Add」をクリックして、b)「pan agent」を追加します。
 c)「Pan agent」の Permissions で以下のように「Enable Account」、「Remote Enable」、「Read Security」にチェック を入れて、d)「OK」をクリックします。

Security for ROOT\CIMV2
Security
Group or user names:
& Authenticated Users
pan agent (panagent@acme.com) b)
Administrators (ACME¥Administrators)
a) Add Remove
Permissions for pan agent Allow Deny
Provider Write
Enable Account
Remote Enable
Fdit Security
click Advanced.
d) OK Cancel Apply

13.1.2. PA Firewall の設定

(1) a)「Network」 \rightarrow b)「ゾーン」で表示された c)「Trust」をクリックします。

🛲 paloalto								_	_
NETWORKS®	Dashboard	ACC Monitor	Policies Objects	Network	Device			▲ コミット	省 🧠 Config 🔻 🔍 検索
									ら @ヘルプ
ゴインターフェイス	٩								2 個の項目s 🏓 🗶
								ユーザー	· ID
- パーチャル ワイヤー	🔲 名前 🔺 タイプ	インターフェイス/仮想システム	ゾーン プロテクション プ	ロファイル バ	ペケット バッファ保護	ログ設定	有効	含まれるネットワーク	除外されるネットワーク
🐨 仮想ルーター	Trust C ayer3	ethernet1/2						任意	なし
(PSec トンネル	Untrust layer3	ethernet1/1						任意	なし
T DHCP									

(2) a)「ユーザ ID の有効化」にチェックを入れ、b)「OK」をクリックします。

ゾーン		0
名前	Trust	ユーザー ID ACL a)
タイプ	レイヤー3 マ	■ 許可リスト 🔺
 インターフェイス ▲ ethernet1/2 	s	アドレスまたはアドレス グループを選択するか、自分のアド レスを入力してください。 Ex: 192.168.1.20 or 192.168.1.0/24
		 ● 追加 ● 割除 これらのフドレス/サブネットからのユーザーは特定されます。 ● 除外リスト ▲
●追加●削除		アドレスまたはアドレス グループを選択するか、自分のアド レスを入力してください。 Ex: 192.168.1.20 or 192.168.1.0/24
- ゾーン プロテクション		
ゾーン プロテクション プロファイル	None	
	🦳 パケット バッファ保護の有効化	●追加 ● 割除
		これらのアドレス/サブネットからのユーザーは特定されません。
		b) DK キャンセル

(3) a)「Device」→ b)「ユーザーID」→ c)「ユーザーマッピング」の、「Palo Alto Networks User-ID エージェントの設定」の d) をクリックします。

paloalto	Dashboard AC	C Monitor P	Policies Objects	Network	Device	2	コミット
	Dashboard AC C) ユーザーマッピング Palo Alto Networks User-IDエ	C Monitor P 接続のセキュリティ ージェントの設定 セキュリティ サーバーログのモニ セッシ サーバーセッションの読み Novell eDirectory ク Syslog サービス フロ フロ ユーザー ID タイムアウト ユーザー ID タイ N N	Policies Objects ユーザー ID エージ ログの有効化 タク-頻度(や) 2 タンの有効化 マンリ関隔(や) 30 、プロファイル コーブ関隔(分) 20 本取り頻度(や) 10 マエリ関隔(分) 20 本有効にする イムアウト(分) 45 VTLM ドメイン いコーンク名	Network エント ターミ	Device a) ナルサービス	ミ エージェント グループマッピング設定 全 d)	シコミット
HTTP							

(4) a)「WMI 認証」で、b)AD に登録したユーザ名(ACME/panagent)とそのパスワードを入力し、c)「OK」をクリックします。

Palo Alto Net	works User-IDエージュ	こントの設定				0
WMI 認証	サーバー モニタ	クライアントによるプローブ	キャッシュ	NTLM	再配信	Syslog のフィル・
a)	ユーザー名	ACME\panagent b)				
	パスワード					
	再入力 パスワード					
				C)	ОК	キャンセル

(5) a)「Device」 \rightarrow b)「ユーザーID」 \rightarrow c)「ユーザーマッピング」の、「サーバーモニタリング」の d)「追加」をクリックします。



(6) a)名前に「AD(任意)」、b)タイプは「Microsoft Active Directory」が選択されていることを確認し、c)ネットワークアドレスには、ADのアドレス「192.168.45.65」を入力します。
 d)「OK」をクリックします。

ユーザー ID モニタ	サーバー			0
名前	AD	a)		
内容				
	✔ 有効			
タイプ	Microsoft Active Directory	b)		~
ネットワーク アドレス	192.168.45.65	C)		
	ď		ОК	キャンセル

- (7) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)
- (8) コミット後、状態が「Connected」になれば OK です。

サーバー モニタリング				
名前	有効	タイプ	ネットワーク アドレス	状態
AD	1	Microsoft Active Directory	192.168.45.65	Connected

13.2.動作確認

(1) Windows ドメインに属しているクライアント PC にログインします。

本ガイドでは、「acme¥user1」でログインします。

(2) PA Firewall で、以下のコマンドを実行し、IP アドレスとユーザ名のマッピング状態を確認します。

admin@PA-VM> show user ip-user-mapping all

IP	Vsys	From	User	IdleTimeout(s)	MaxTimeout(s)
192. 168. 45. 20	vsys1	AD	acme¥panagent	1895	1895
192.168.45.32 Total: 3 users	vsys1	AD	acme¥user1	1659	1659

(3) クライアント PC の Web ブラウザで、インターネット上のいくつかの Web サイトへアクセスします。

(4) a)「Monitor」→ b)「トラフィック」でログを確認します。

送信元ユーザーのフィールドに「ドメイン¥ユーザ名」が表示されます。

paloalto		Deathered	100	Manifest	Dellater	Objects	Network	Device					\$ ¬ >
NETWORKS ¹		Dashboard	AUU	a)	Policies	Objects	Network	Device					 ₹
	٩												
- (1)		受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	IP プロトコル	宛先ポート	アプリケーション	アクション	ルール
😺 URL フィルタリング	Þ	03/19 19:17:29	drop	Trust	Untrust	192.168.45.32	acme\user1	4.2.2.2	icmp	0	ping	deny	interzone-default
Real WildFireへの送信	P	03/19 19:17:26	end	Trust	Untrust	192.168.45.11	acme\panagent	199.167.52.141	tcp	443	paloalto-updates	allow	allow outbound web
Image: Imag	D	03/19 19:17:25	drop	Trust	Untrust	192.168.45.32	acme\user1	172.217.25.65	udp	443	not-applicable	deny	interzone-default
III ユーザー ID	D	03/19 19:17:24	drop	Trust	Untrust	192.168.45.32	acme\user1	172.217.25.65	udp	443	not-applicable	deny	interzone-default
🚵 トンネル検査		03/19 19:17:23	drop	Trust	Untrust	192.168.45.32	acme\user1	74.125.106.102	udp	443	not-applicable	deny	interzone-default
 設定 システム 	D	03/19 19:17:23	drop	Trust	Untrust	192.168.45.32	acme\user1	172.217.25.65	udp	443	not-applicable	deny	interzone-default
R 75-4	D	03/19 19:17:22	drop	Trust	Untrust	192.168.45.32	acme\user1	4.2.2.2	icmp	0	ping	deny	interzone-default
	D	03/19 19:17:22	drop	Trust	Untrust	192.168.45.32	acme\user1	172.217.25.65	udp	443	not-applicable	deny	interzone-default
■ 統合済み	D	03/19 19:17:22	drop	Trust	Untrust	192.168.45.32	acme\user1	172.217.25.65	udp	443	not-applicable	deny	interzone-default
マロアプリケーション スコープ	D	03/19 19:17:22	drop	Trust	Untrust	192.168.45.32	acme\user1	172.217.25.65	udp	443	not-applicable	deny	interzone-default
サマリー	P	03/19 19:17:21	drop	Trust	Untrust	192.168.45.32	acme\user1	74.125.106.102	udp	443	not-applicable	deny	interzone-default

13.2.2. User-ID 連携が動作しない場合

設定の見直しに加えて、以下の2点を確認してください。

(1) AD と PA Firewall の時刻を確認してください。

AD と PA Firewall での時刻ずれは、5 分以内に収まっている必要があります。 どちらも NTP で同期ができていることが望ましいです。

(2) Windows Firewall を確認してください。

Windows Firewall によってブロックされている可能性があります。 「Server Manager」→「Local Server」で表示されます。 切り分け作業として、一時的に OFF にして、確認してみてください。

b		Server Manager
Server Ma	nager • Local Se	erver
📰 Dashboard	For Win2012	
Local Server	Completion	W6-2012
All Servers	Computer name Domain	acme.com
🖳 AD CS		
AD DS		
🔗 DNS	Windows Firewall	Domain: Off
■ File and Storage Services ▷	Remote management	Enabled
	Remote Desktop	Enabled
N 113	NIC Teaming	Disabled
	Ethernet0	192.168.45.65, IPv6 enabled

User-ID 連携は、AD 以外にも LDAP や Wi-Fi 認証サーバーなど、様々な認証基盤との連携が可能です。 その他の連携方法については、ご購入元の弊社パートナー様へお問い合わせください。 14. おわりに

基本的な PA Firewall の設定方法に関しては以上です。

パロアルトネットワークスでは、PA Firewall 及び Wildfire (サンドボックス) だけでなく、未知の脅威を防御することに主 眼を置いた次世代エンドポイントセキュリティ「Traps」を交えた、トータルなセキュリティソリューション: 「次世代セキュリティプラットフォーム」を展開しています。

さらに、ログ及びコンフィグの集中管理を行うPanorama、セキュリティイベント調査をより効率化する AutoFocus、SaaS セキュリティに特化した Aperture などによって、パロアルトネットワークスが、皆様のネットワークが抱える様々なセキュリティの課題を包括的に解決することができます。

これらの具体的な内容に関しては、弊社にお気軽にお問合せください。

また本ガイドに記載されていない PA シリーズの設定方法に関するより詳細が必要な場合は、各種 WEB サイトにてご確認いただくか、ご購入元にお問い合わせください。

<パロアルトネットワークス WEB サイトの紹介>

パロアルトネットワークス総合サイト https://www.paloaltonetworks.jp/

ナレッジベース総合サイト(英語) https://support.paloaltonetworks.com/

ライブコミュニティ(英語・一部日本語) https://live.paloaltonetworks.com/

以上

パロアルトネットワークス株式会社 〒102-0094 東京都千代田区紀尾井町4番3号 泉館紀尾井町3F

本資料はパロアルトネットワークスのエンジニアが特定のソフトウェアバージョンの動作仕様に基づいて作成した構築・設計を補助するための資料であり、 メーカー公式資料とは異なります。資料の記載内容に誤りがあった際には指摘に基づいて修正を行いますが、内容についての責任は一切負いません。 また、修正、変更、改訂は予告無く行われます。 URL カテゴリは、66 種類となっています(2018/3 現在)。

本ガイド内で設定したものは、B:ブロック、C:コンティニュー、A:アラートに「1」を入れています。 カテゴリ説明を参照頂き、必要に応じて、自社の PA Firewall のブロック/コンティニュー/アラートに追加してください。

No.	В	С	Α	URL カテゴリ名		カテゴリ説明		
1				Abortion	(人口中絶)	中絶に反対または賛成、中絶手続きに関する詳細、中絶を援助またはサ ポートするフォーラムに関する情報やグループのサイト、中絶推進の結果/ 効果に関する情報を提供するサイト。		
2	1			Abused Drugs	(乱用薬物)	合法および非合法を問わず薬の乱用を促進するサイト、薬物関連の道具 の使用や販売、薬の製造や販売に関連するサイト。		
3		1		Adult	(アダルト)	性的に露骨な内容、文章(言葉を含む)、芸術、または本質的に性的表現 がきわどい製品、オンライングループやフォーラム。ビデオチャット、エスコ ートサービス、ストリップクラブを含むアダルトサービスを宣伝するサイト。 ゲームやコミックであれアダルトコンテンツを含むものはすべて adult にカ テゴリ化される。		
4				Alcohol and Tobacco	(アルコールとタバコ)	アルコールやたばこ製品、関連用品の販売、製造、使用に関連するサイト。		
5				Auctions	(オークション)	個人間での商品売買を促進するサイト。		
6				Business and Economy	(ビジネスと経済)	マーケティング、経営、経済、起業や事業経営に関するサイト。広告・マー ケティング企業も含まれます。企業サイトは、各企業の分野で分類される べきで、このカテゴリに含むべきではない。fedex.com や ups.com といっ た運送サイトが含まれる。http://cox.net と http://directv.com はケーブル 会社であり、"business and economy" でなければならない(タイムワー ナーケーブルとコムキャストも同様)。ストリーミング用に個別のサイトがあ る場合(コムキャストでは xfinity.comcast.net)、"streaming media" カテ ゴリとする。		
7	1			Command and Control	(コマンドとコントロー ル)	マルウェアまたは侵害されたシステムが使う URL やドメイン。 それらの感染システムが、不正コマンドを受信するためや、データを送信 することを目的として、攻撃者のリモートサーバーへ密かに通信する際に 利用する宛先。		
8				Computer and Internet Info	(コンピュータとインタ ーネット情報)	コンピュータとインターネットに関する一般的な情報。コンピュータサイエン ス、エンジニアリグ、ハードウェア、ソフトウェア、セキュリティ、プログラミン グなどに関するサイトも含まれる。プログラミングは reference と重複する かもしれないが、メインカテゴリは computer and internet info となる。		
9				Content Delivery Networks	(コンテンツ配信ネット ワーク)	広告、メディア、ファイルなどのようなコンテンツを第三者に配信することを 主に行うサイト。画像サーバーを含む。		
10	1			Copyright Infringement	(著作権侵害)	著作権を侵害したビデオや映画、その他のメディアファイルをダウンロード により提供する専用のウェブサイトやサービス。		
11		1		Dating	(出会い系)	出会い系、オンラインデートサービス、アドバイス、その他個人的な広告を 提供するウェブサイト。		
12	1			Dynamic DNS	(ダイナミック DNS)	提供されたまたは動的なドメイン名と IP アドレスを関連付けるためにダイ ナミック DNS サービスを利用しているサイト。ダイナミック DNS サイトは、 サイバー攻撃者に対する C&C 通信および、他の悪意のある目的のため に使用される場合がある。		
13				Educational Institutions	(教育機関)	学校、短期大学、大学、学区、オンラインクラス、その他の学術機関用の 公式 Web サイト。小学校、高校、大学など大規模な制定された教育機関 を指す。個別指導塾もこのカテゴリとなる。		
14				Entertainment and Arts	(娯楽と芸術)	映画、テレビ、ラジオ、ビデオ、プログラミングガイド・ツール、マンガ、芸 能、博物館、アートギャラリーのサイト。エンターテインメント、有名人、業 界のニュースに関するサイトも含まれる。		
15	1			Extremism	(過激主義・思想)	テロや人種差別、ファシズムや人種、異なる民族的背景、宗教や信仰を判 別する過激主義・思想を促進するウェブサイト。		
16				Financial Services	(金融サービス)	オンラインバンキング、ローン、住宅ローン、債務管理、クレジットカード会 社、保険会社などの個人金融情報やアドバイスに関する Web サイト。株 式市場、証券会社、取引サービスに関するサイトは含まれない。外国為替 取引関連サイトを含む。		

No.	В	С	Α	URL カテゴリ名		カテゴリ説明
17		1		Gambling	(ギャンブル)	本物または仮想のお金の交換を容易にする宝くじやギャンブルの Web
				-	· ,	サイト。賭けのオッズやプールに関する情報、ギャンブルに関する指導や
						助言を提供するサイト。ギャンブルを行わないホテルやカジノの企業サイト
						は Travel にカテゴリ化される。
18		1		Games	(ゲーム)	ビデオやコンピュータゲームをオンライン再生やダウンロードできるサイ
						ト、ゲーム批評、ヒント、裏技を提供するサイト。非電子ゲームの教育、ボ
						ードゲームの販売や交換、関連する出版物やメディアに関するサイト。オ
						ンライン懸賞や景品を扱うサイトを含む。
19				Government	(政治)	地方自治体、州政府、国家政府の公式 Web サイト。関係機関、サービ
						ス、法律に関するサイトを含む。公共図書館は除く。
20		1		Hacking	(ハッキング)	通信機器やソフトウェアに対して、違法または疑わしいアクセスや利用に
						関するサイト。ネットワークやシステムが侵害される可能性のあるプログラ
						ムの開発や配布、手順の助言やヒントに関するサイト。また、ライセンスや
						デジタル著作権システムをバイパスさせるサイトも含まれる。
21				Health and	(健康と医療)	一般的な健康に関する情報、問題、伝統医学や現代医学の助言、治癒、
				Medicine		治療に関する情報を含むサイト。さまざまな医療分野、慣行、設備、専門
						家のためのサイトが含まれる。医療保険、美容整形に関するサイトも含ま
						れる。動物病院を含む。
22				Home and	(住まいと庭)	住まいの修繕や管理、建築、設計、建設、装飾、ガーデニングに関する情
				Garden		報、製品、サービスを提供するサイト。
23				Hunting and	(ハンティングとフィッ	狩猟や釣りの情報、説明、販売、関連装置や関連用品に関するサイト。
				Fishing	シング)	
24			1	Insufficient	(識別困難な Web サ	テストページやコンテンツが存在しない場合やユーザ向けではない API ア
				Content	イト)	クセス用のサイト、コンテンツの表示に認証必要などカテゴリ分類が困難
						な Web サイト。
25				Internet	(インターネット通信と	ビデオチャット、インスタントメッセージ、電話機能のサービスをサポートま
					電話)	たは提供するサイト。
26				Internet Portals	(ポータルサイト)	通常 広筋たコンテンツやトピックをまとめることでユーザーに対して閉始
20					(//)//////////////////////////////////	通市、公配なコンプングやドビブジをよこのることでユーダーに対して開始 占とたるサービスを提供するサイト
27				Joh Cooroh		
21				Job Search	(珮探し)	水入情報や雇用評価、面接のアトハイスやビント、雇用土と候補者の両方 に対する関連サービュに関するサイト
					() ± (†)	
28				Legai	(法律)	法律、法律サービス、法律事務所、その他法律関連の問題に関する情
						戦、分析、助言に関するサ1ト。
29	1			Malware	(マルウェア)	悪意あるコンテンツ、実行可能ファイル、スクリプト、ウイルス、トロイの木
						馬、コードを含むサイト。
30				Military	(軍事)	軍事部門、軍人募集、現在や過去の作戦、関連道具に関する情報や解説
						のサイト。
31				Motor Vehicles	(モータービークル)	自動車、オートバイ、ボート、トラック、RV に関して批評、販売、取引、改
						造、部品、その他関連する議論に関する情報。
32				Music	(音楽)	音楽の販売、配布、情報に関するサイト。音楽アーティスト、グループ、レ
						ーベル、イベント、歌詞、音楽ビジネスに関するその他の情報に関する
						Web サイトを含む。動物病院を含む。
33				News	(ニュース)	オンライン出版物、ニュースワイヤー(オンラインでニュースを送受信する
						システム)サービス、その他、現在のイベント、天候、時事問題を集約した
						サイト。新聞、ラジオ局、雑誌、ポッドキャストを含む。reddit, delicious,
						digg のようなソーシャルブックマークサイトを含む。
34			1	Not-resolved	(未解決)	Web サイトがローカル URL フィルタリングデータベースに見つからず、フ
						アイアウォールが、カテゴリをチェックするためにクラウドデータベースに接
						続を試みたが、接続できなかった状態を示す。
						UDL カニゴリの会昭が史にされても、DA Firowall はいての順で於声たに
						URL カナゴリの参照が美行されると、PA Filewall は以下の順で検索を打
						ン。 ① データプレーンの URL キャッシュをチェック
						\odot クロン URL キャッシュをチェック ② 管理プレーンの URL キャッシュをチェック
						クラウド内の URL データベースへ問い合わせる。
35				Nudity	(裸体)	作品として性的な意図や意味があるかによらず、人体のヌードやヤミヌー
					(POLLY	ドを含むサイト。参加者の画像を含むヌーディストやヌーディストサイトも含
						まれる。

No.	В	С	Α	URL カテゴリ名		カテゴリ説明
36				Online Storage	(オンラインストレージ	ファイルの無料オンラインストレージをサービスとして提供する Web サイ
				and Backup	とバックアップ)	ト。flickr.com や shutterfly.com のような写真共有サイトを含む。
37	1			Parked	(パークドメイン)	限られたコンテンツやクリックスルー広告をホストする URL。ホストに対し
						て収入を生むことがあるが、一般にはエンドユーザにとって有用なコンテ
						ンツやサイトか含まれていない。工事中のサイトやフォルタのみのペーン
38	1			Peer-to-Peer	(ピアツ―ピア)	とさい。 ターゲットファイルへのデータ ダウンロードレナプログラム メディアファイ
00	•					ル、その他ソフトウェアアプリケーションへのピアツーピア共有アクセスま
						たはクライアントを提供するサイト。シェアウェアやフリーウェアサイトは含
						まない。bittorrent ダウンロード機能を持つサイトが主に含まれる。
39				Personal Sites	(個人サイトとブログ)	個人やグループによる、私的な Web サイトやブログ。最初のコンテンツに
				and Blogs		基づいて分類されるべき。たとえば誰かがクルマについてのブログを持っ
						ている場合は、そのサイトは"motor vehicles"に分類されるべきである。サ
						イトが純粋なフログである場合は、" Personal Sites and Blogs " となりま ナ
40				Philosophy and	(折受と政策支援)	9。 折学や政治的目留に関する信報 祖占やキャンペーンを含むサイト
40				Political	\ロナこ以來又抜)	ロナ に以れれれた時にはッ の時秋、沈点 ドインハーンを召む リイト。
				Advocacy		
41	1			Phishing	(フィッシング)	フィッシングやファーミングによりユーザーから個人情報を取得する、見か
						「「上は信頼でさそうなサイト。
42				Private IP Addresses	(ブライベート IP アドレ っ)	このカテゴリには RFC1918 "Address Allocation for Private Intranets"
				/ 100103003	^)	じ正我されに IP プトレスを召む。 10 0 0 0 - 10 255 255 255 (10/8 プレフィックス)
						172.16.0.0 - 172.31.255.255 (172.16/12 プレフィックス)
						192.168.0.0 - 192.168.255.255 (192.168/16 プレフィックス)
						169.254.0.0 - 169.254.255.255 (169.254/16 プレフィックス)
						また*.local のような公共の DNS システムに登録されていないドメインが
					<u> </u>	含まれる。
43	1			Proxy Avoidance	(プロキシ回避と匿名	プロキシサーバーやその他方式で URL フィルタリングや URL 監視をバ
				Anonymizers	70+2)	1//~9 & 71F.
44	1			Questionable	(疑わしいサイト)	下品なユーモア、特定層の個人やグループをターゲットにした不快なコン
						テンツ、犯罪行為、違法行為、手早く金持ちになれる、といったものを含む
45				Pool Estato	(丁卦主)	サイト。 て私立任代 旺吉 明はせているりはおに明せてせ ハーて私立業者 人
40				Real Estate	(个刬生)	个 動 生 貝 貝 、 販 元 、 民 定 9 の ワ 1 ト ・ ト 5 、 ・ ・ ・ ・ ・ ・ ・ ・
46				Recreation and	(しクリエー・ションと趣	レクリエーションや趣味に関する情報、フォーラム、団体、グループ、おと
-10				Hobbies	(ビノリエーンヨンC歴 味)	び出版に関するサイト。
47				Reference and	(参考と調査)	個人、専門家、学術系のリファレンスポータル、コンテンツ、サービス。オン
				Research		ライン辞書、地図、年間、国勢調査、図書館、系譜、科学情報が含まれ
						る。公共図書館であれば.gov で終わるサイトも含む。
48				Religion	(宗教)	各種宗教、関連活動やイベントに関する情報。宗教団体、関係者や礼拝
						場所に関する Web サイトを含む。占星術、星占い、占いに関するサイトを
40				Sooroh Enginoo	(サーイエンパン)	含む。 オーロード フレーズ てのゆポニオ カナは田レイやま ハーク・フェノスナ
49				Search Engines	(サーチエノシノ)	キー・フート、フレース、その他ハフメーダを使用して使業インダーフェイスを 焊供するサイト 検索結果と! て情報 ウェブサイト 両角 ファイルを返
						近氏するり 11°。 快来相来として 11秋、 ウエン り 11、 画像、 ファイルを 医す。
50				Sex Education		- ~ 生殖、性的発育、安全な性行為慣行、性病、避妊、より良いセックスに関
						する情報、関連する製品や道具に関する情報。関係するグループ、フォー
						ラムや組織のためのウェブサイトを含む。
51				Shareware and	(シェアウェアとフリー	無料または寄付を受け付けるソフトウェア、スクリーンセーバー、アイコン、
				Freeware	ウェア)	壁紙、ユーティリティ、着メロ、テーマ、ウィジットへのアクセスを提供する
						サイト。また、オーフンソースフロジェクトが含まれる。
52				Shopping	(ショッピング)	商品やサービスの購入を促進するサイト。オンライン小売業者、百貨店、
						小売店、カタロク販売のWebサイト、価格を集約してモニタするサイトも 合まれて、ニニに記載されていてサイルは、さまざさか辛ロを旺ませてい。
						日まれいる。 ニニー 記載され しいるサイトは、 さまさまな問品を販売するオン ライン 商店 またけまた日的がオンラインセール. マです オンライン. 哮 1 た
						アーン回信、みには上な日間がカンフィンビールへてす。カンフィン購入を可能にする化粧品会社のWebページは cosmetics ではなく shonning
						に分類される。食料品店のサイトも含まれる。
No.	В	С	Α	URL カテゴリ名		カテゴリ説明
-----	---	---	---	-----------------------	-------------	---
53				Social	(ソーシャルネットワー	ユーザーが互いにメッセージや写真を投稿したり、人々のグループとコミ
				Networking	キング)	ュニケーションしたりするユーザーコミュニティやサイト。ブログや個人サイ
						トは含まれない。
54				Society	(社会)	一般住民に関連するトピック、ファッション、美容、慈善団体、社会、または
						子供など多種多様な人々に影響のある論点に関するサイト。子供向けに
						作成された Web サイトを含む。子供向けに作成された Web サイトを含
						む。レストラン、UFO に関するサイトを含む。
55				Sports	(スポーツ)	スポーツイベント、選手、コーチ、関係者、チームや団体、スポーツのスコ
						ア、スケジュール、関連ニュース、関連用具に関する情報。ファンタジース
						ポーツや仮想スポーツリーグに関するサイトも含まれる。 ペイントボール
						や各種武道といったスポーツも含まれる。
56				Stock Advice	(株式情報とツール)	株式市場に関する情報、株式やオプション取引、ポートフォリオ管理、投
				and Tools		資戦略、相場、関連ニュースに関する情報。
57				Streaming Media	(ストリーミングメディ	無料または有料のストリームオーディオまたはストリームビデオコンテンツ
					ア)	サイト。テレビ局の Web サイトは entertainment and arts にカテゴリ化さ
						れる。オンラインラジオ局やその他ストリーミング音楽サービスを含む。
58				Swimsuits and	(水着と下着)	水着や下着、その他きわどい衣服の情報や画像を含むサイト
				Intimate Apparel	(
59				Training and	(トレーニングとツー	オンライン教育とトレーニング、関連資料を提供するサイト。自動車教習
				Tools	ル)	所、職業研修などを含めることができる。学習塾や試験対策は技術的に
						は training and tools となる。
60				Translation	(翻訳サイト)	ユーザー入力や URL 翻訳の両方を含む翻訳サービスを提供するサイト。
						これらサイトは、目的ページのコンテンツが翻訳 URL の一部に表示され
						るものとして、ユーザーにフィルタリング回避させることもできます。
61				Travel	(旅行)	旅行の助言、お得な情報、価格情報、旅先情報、観光、関連サービスに
						関する情報のサイト。ホテル、現地の観光スポット、カジノ、航空会社、ク
						ルージング、旅行代理店、レンタカーに関して価格情報や予約ツールを提
						供するサイトを含む。エッフェル塔、グランドキャニオン、テーマパーク、動
						物園、国立公園などの現地観光スポットに関するサイトを含む。タクシー
						会社を含む。
62			1	Unknown	(未知)	Web サイトはまだ分類されていないため、PA Firewall の URL フィルタリ
						ングデータベースまたは URL クラウドデータベースには存在しないことを
						示す。
63		1		Weapons	(武器)	兵器やその使用に関する、販売、批評、説明、取扱のサイト。
64				Web Advertisements	(ウェブ広告)	広告、メディア、コンテンツ、バナーが含まれる。
65				Web Hosting	(ウェブホスティング)	Web 開発、出版、販売促進、トラフィックを増やすためのその他方法に関
						する情報を含む、無料または有料の Web ページのホスティングサービ
						ス。
66				Web-based	(ウェブメール)	電子メールの受信ボックスへのアクセスを与えるか、電子メールを送受信
				Email		できる Web サイト。