



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

Palo Alto Networks K.K.
2018/4

目次

1. はじめに	4
2. ネットワーク構成	5
3. 初期設定	6
3.1. マネージメント IP の設定	6
3.2. WEBUI へのアクセス	7
3.3. DNS と NTP の設定	9
3.4. 設定のコミット	11
3.5. ライセンス投入	12
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	18
4. ネットワーク設定	21
4.1. VIRTUAL WIRE 設定の削除	21
4.2. ゾーンの設定	22
4.3. インターフェイスの設定	23
4.4. ルーティング	26
5. NAT	28
6. 全許可ポリシーの設定	30
6.1. [参考]「ルールの使用状況」カウンター	30
6.2. 設定	31
6.3. 通信確認	33
7. SSL/TLS 復号化の設定	34
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ポート	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	65
9.2. マネージメントインターフェイスの設定変更	66
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. サービスを限定するポリシーの設定	70
10.1. HTTP と HTTPS のみ許可する設定	70
10.2. INTERZONE-DEFAULT の設定変更	74
11. APP-ID	75
11.1. DNS を許可する	75
11.2. [参考] APPLICATION-DEFAULT とは	79
11.3. NTP を許可する	80
11.4. YOUTUBE を拒否する	82
11.5. 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	89
11.7.	リスク5のFILE SHARINGをまとめて拒否する	91
11.8.	リスク5のFILE SHARINGのうち、一つだけ許可する.....	96
12.	CONTENT-ID	99
12.1.	アンチウイルス	99
12.2.	脆弱性防御.....	103
12.3.	WILDFIRE	107
12.4.	ファイルブロッキング	111
12.5.	アンチスパイウェア	115
12.6.	URL フィルタリング	122
12.7.	データフィルタリング	130
13.	USER-ID	134
13.1.	設定.....	134
13.2.	動作確認	139
14.	おわりに.....	141
15.	[参考] URL カテゴリの一覧	142

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。

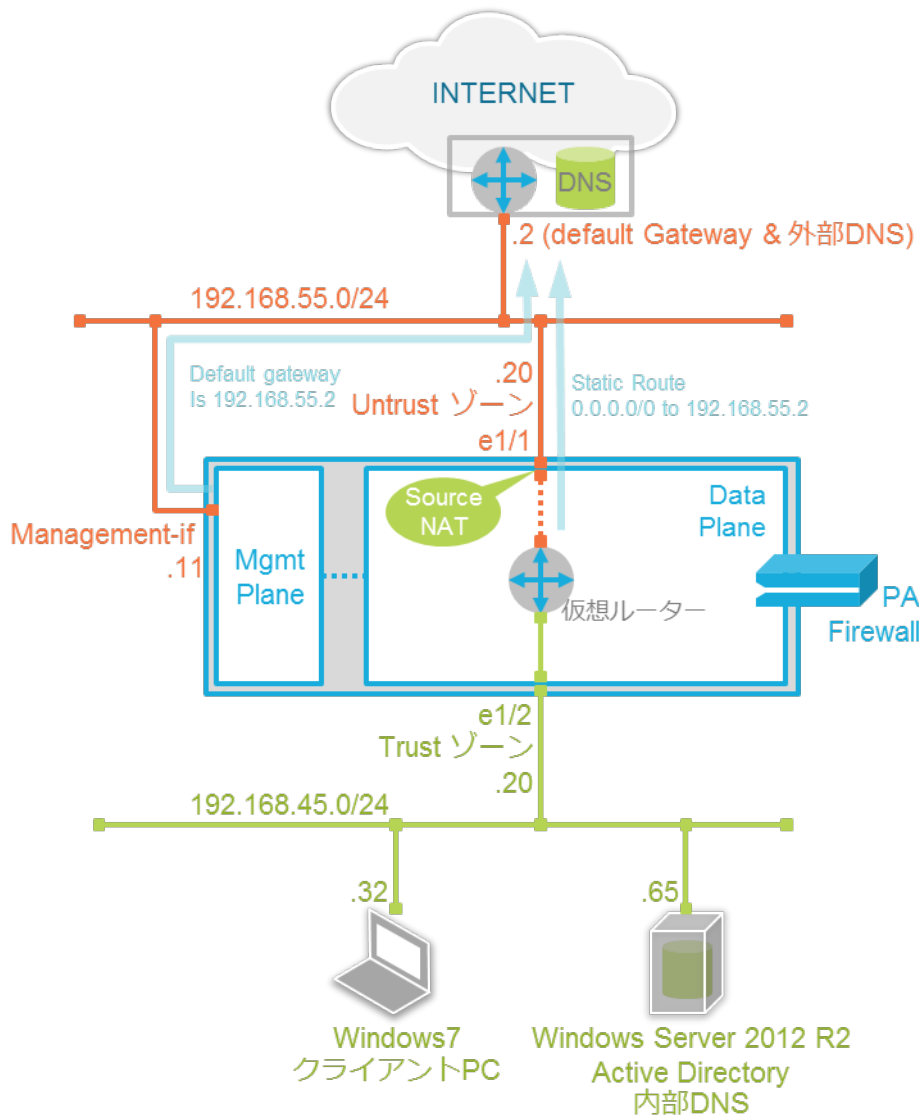
- ① App-ID アプリケーションを識別
- ② Content-ID コンテンツを識別
- ③ User-ID ユーザーを識別

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。
 - 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なります。
- 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 prompt  
... 75%98%. . . . . 100%  
Configuration committed successfully
```

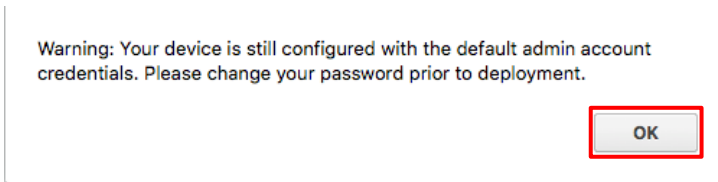
```
[edit]  
admin@PA-VM#
```

3.2. WebUI へのアクセス

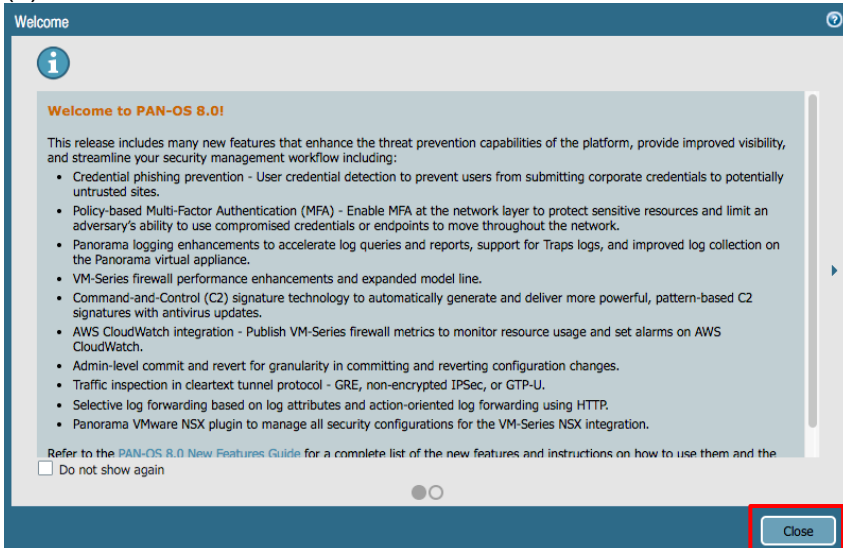
- (1) マネージメントインターフェイスが接続されたネットワーク上のコンソール用 PC から、ブラウザで <https://192.168.55.11> へアクセスします。
- (2) 証明書の警告がでますが、そのままアクセスしてください。
- (3) 認証画面が出ますので、「ユーザ名: admin、パスワード: admin」を入力し、「Log In」ボタンを押します。



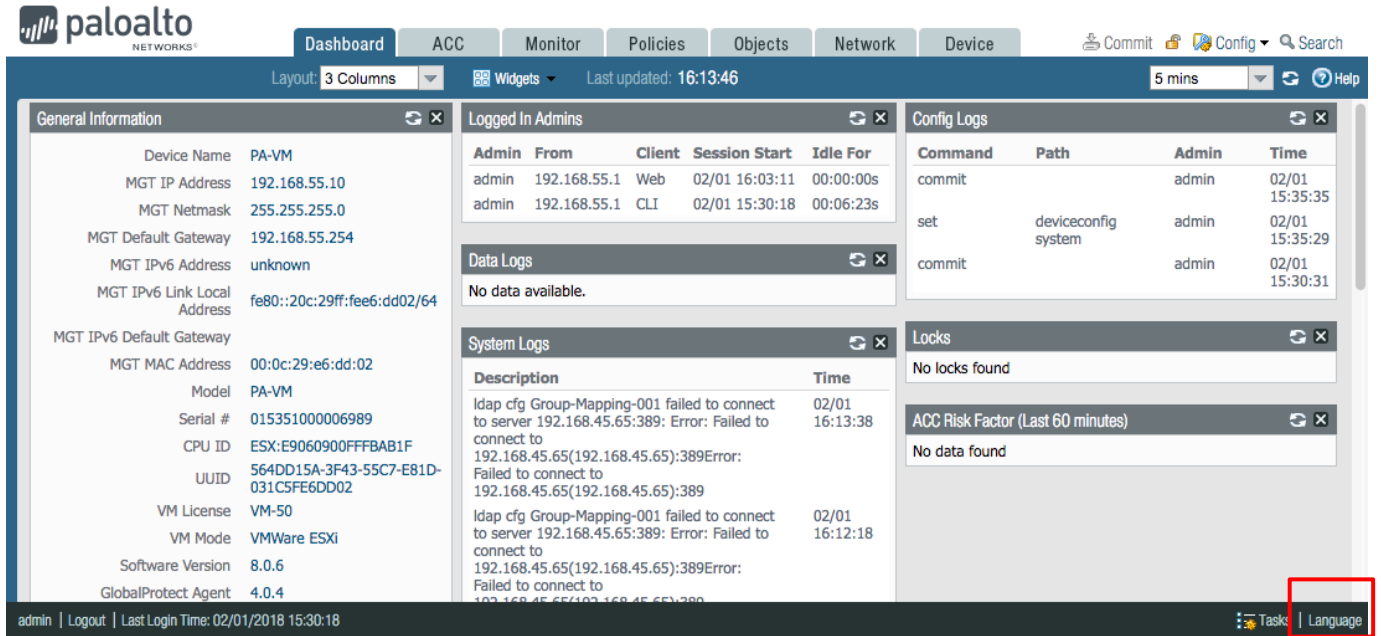
- (4) Admin アカウントのパスワードをデフォルトのまま利用していることに関する警告がでます。「OK」を押します。



- (5) Welcome 画面が出ます。「Close」をクリックします。



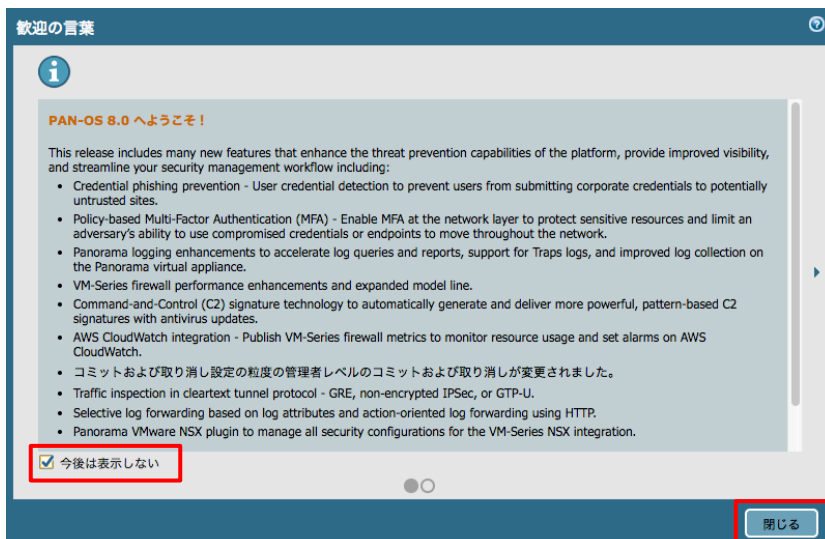
- (6) ダッシュボード画面が表示されます。
以降、日本語のスクリーンショットを使っているのので、日本語へ切り替えます。
右下にある、「Language」をクリックします。



- (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。




- (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。



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) 「Device」 → b) 「セットアップ」 → c) 「サービス」 → d)  アイコンをクリックします。



(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。



(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。

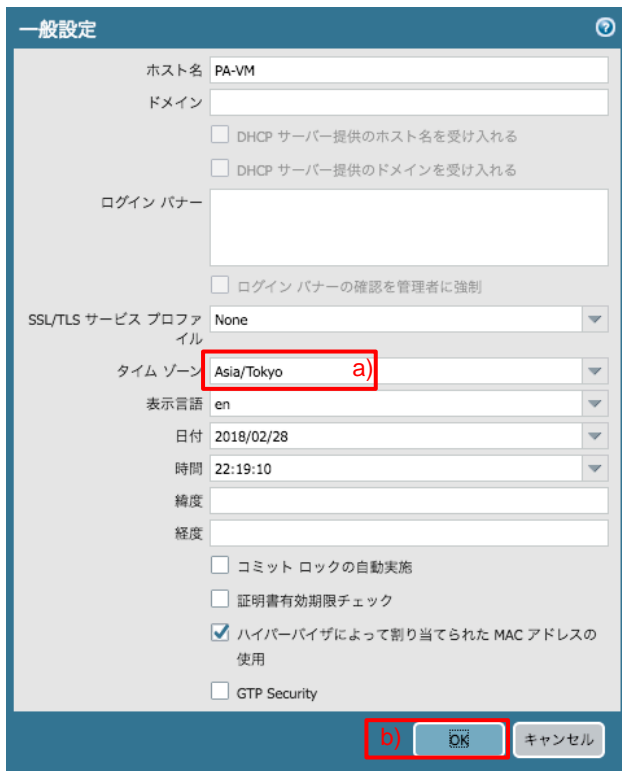


(4) タイムゾーンを日本に変更します。

a)「Device」 → b)「セットアップ」 → c)「管理」 → 「一般設定」の d)  アイコンをクリックします。



(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。



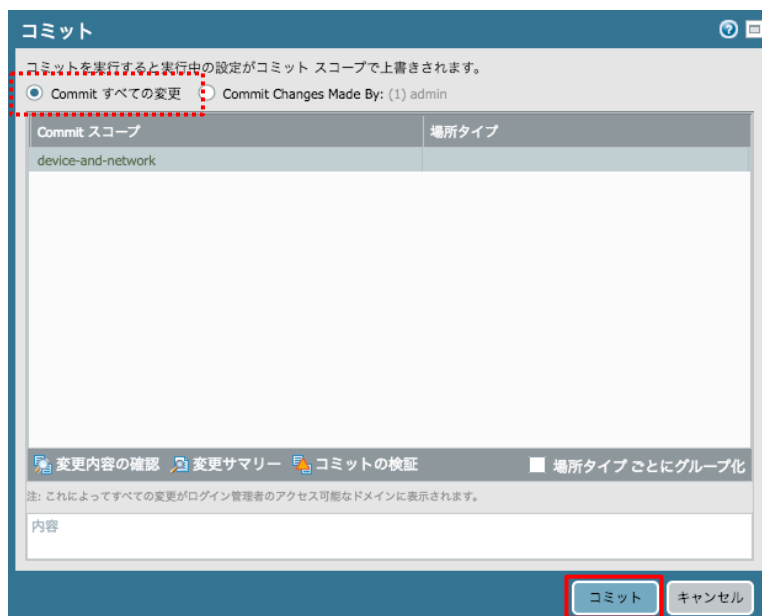
3.4. 設定のコミット

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。



(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

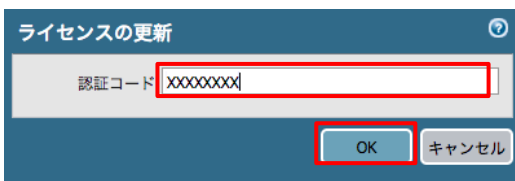
サポートライセンスの投入ステップです。

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。



- (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。

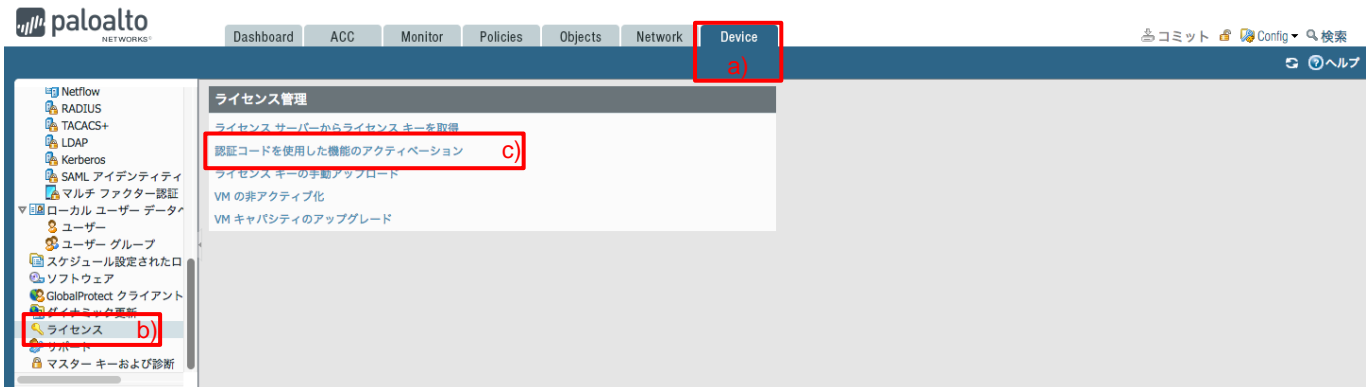


3.5.2. 機能ライセンス

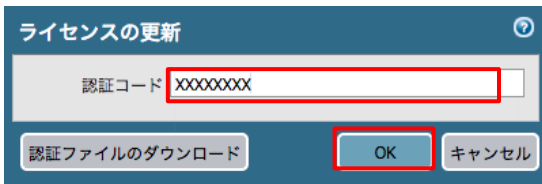
各機能のライセンス投入ステップです。

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。



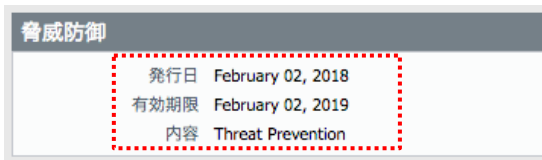
(2) 認証コード(ライセンス証書に記載された Auth Code)を入力して、「OK」をクリックします。



(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。

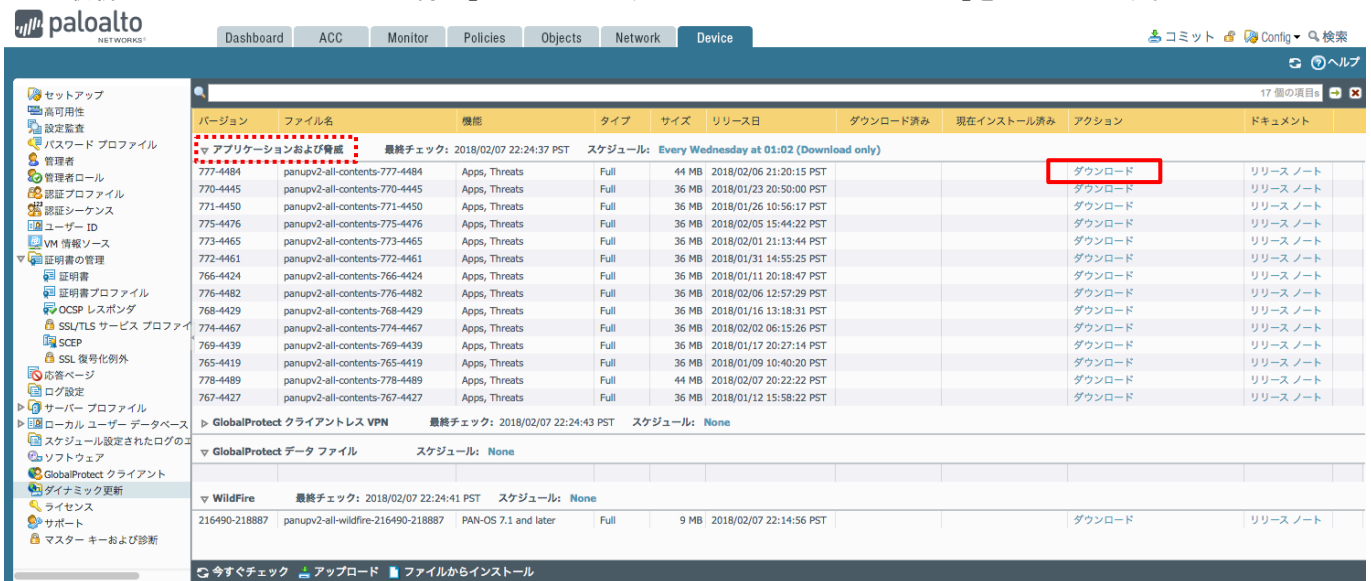
3.6.1. ダイナミック更新

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。

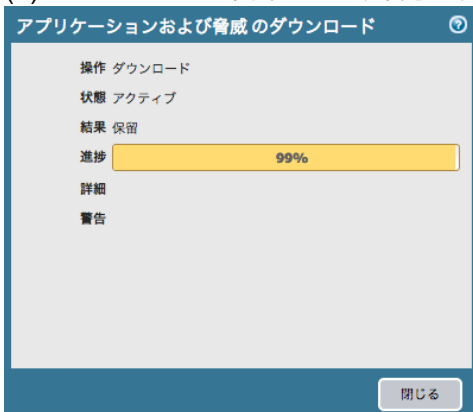
(1) a) 「Device」 → b) 「ダイナミック更新」 → c) 「今すぐチェック」をクリックします。



(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。



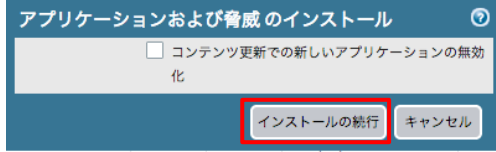
(3) ダウンロードが開始されます。完了するまで待ちます。



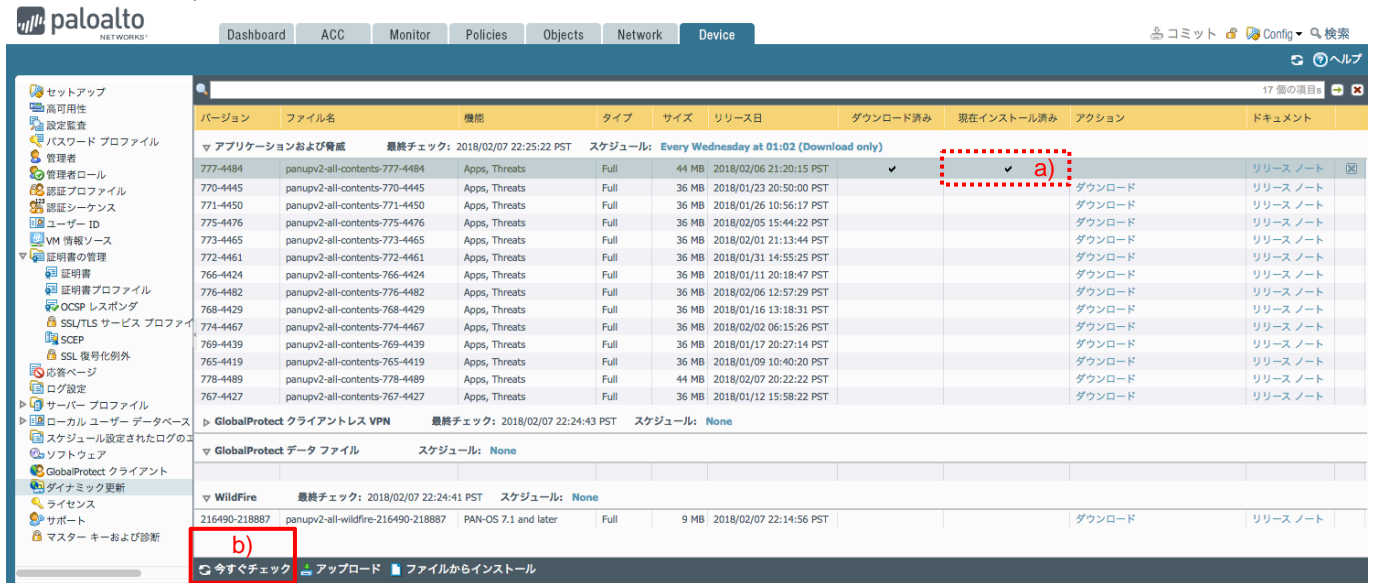
(4) アクション列の「インストール」をクリックします。



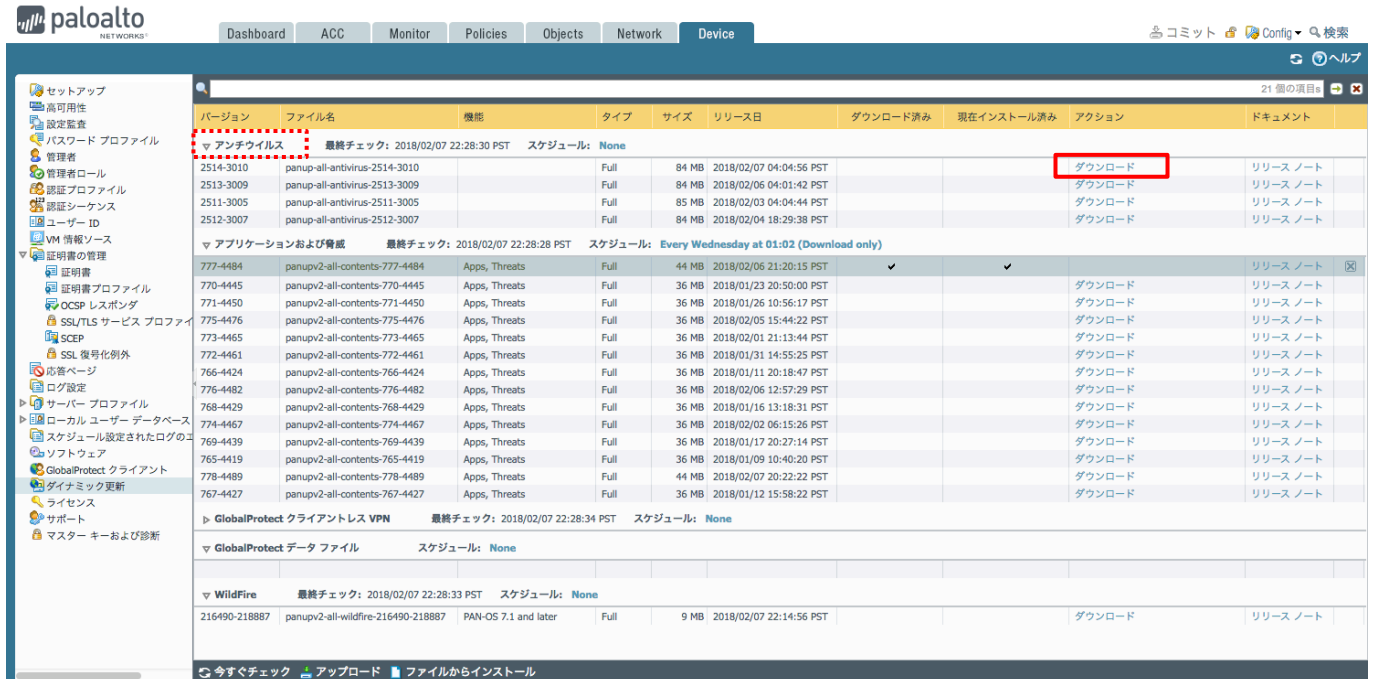
(5) 「インストールの続行」をクリックします。



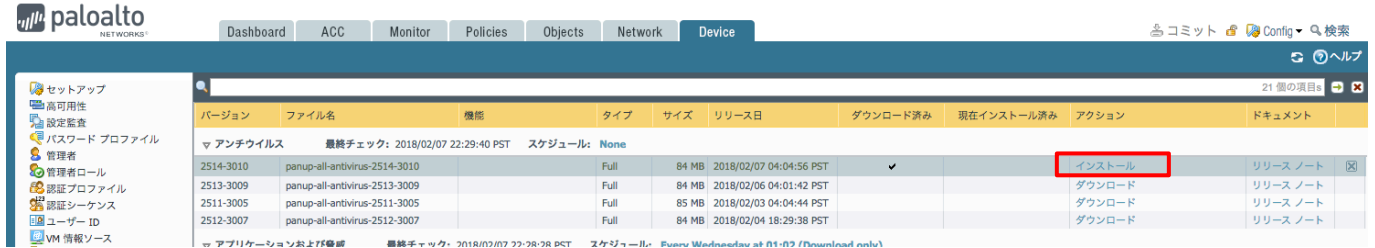
(6) インストールが完了すると、a)現在インストール済み列にチェックが入った状態になります。もう一度、b)「今すぐチェック」をクリックします。



(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。



(8) アクション列の「インストール」をクリックします。

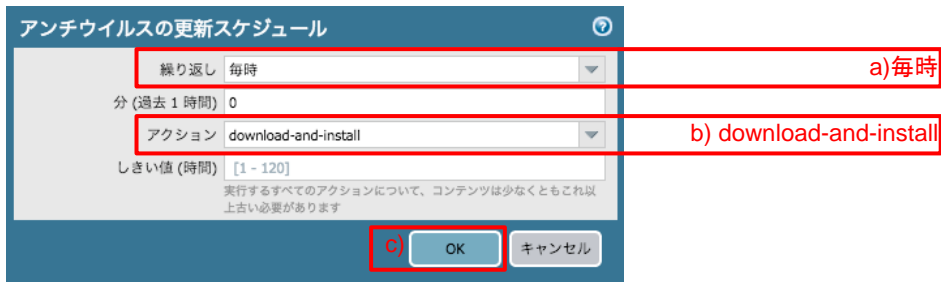


(9) インストールが完了すると、a) 「現在インストール済み」列にチェックが入った状態になります。

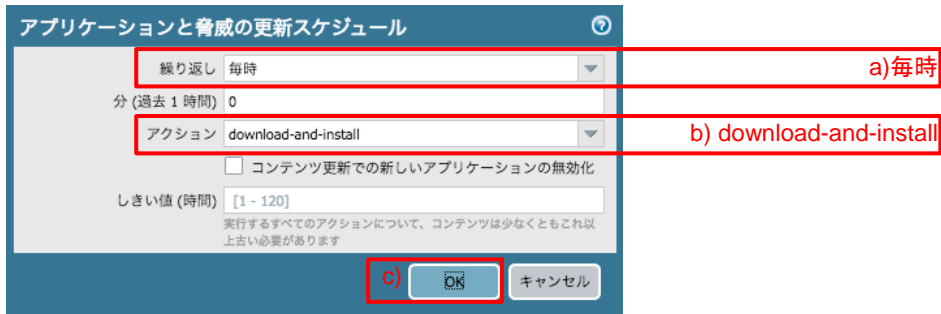
シグネチャの自動インストールの設定を行います。 b)「スケジュール: None」をクリックします。



(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。



(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。



(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。



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

The screenshot shows the Palo Alto Networks management interface. The 'Device' tab is selected. In the left-hand navigation menu, 'ライセンス' (Licenses) is highlighted with a red box and labeled 'b)'. The main content area displays a list of licenses. The 'PAN-DB URL Filtering' license is highlighted with a red dashed box. Underneath it, the 'ダウンロードの状態' (Download status) is set to 'はい' (Yes), and the '今すぐダウンロード' (Download now) button is highlighted with a red box and labeled 'c)'. Other licenses shown include PA-VM, BrightCloud URL Filtering, GlobalProtect ポータル, Premium, and WildFire License.

(2) 警告が出ますが、「はい」をクリックします。

A warning dialog box with a yellow warning icon. The text reads: 'シード データベースを再ダウンロードすると、現在のキャッシュが新しいシード エントリで上書きされます。続行しますか?' (If you re-download the seed database, the current cache will be overwritten with new seed entries. Do you want to continue?). At the bottom, there are two buttons: 'はい' (Yes) and 'いいえ' (No). The 'はい' button is highlighted with a red box.

(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。

A dialog box titled 'URL フィルタリング データベースのダウンロード' (Download URL Filtering Database). It contains a dropdown menu with 'Japan' selected, highlighted with a red box and labeled 'a)'. Below the dropdown are two buttons: 'OK' and 'キャンセル' (Cancel). The 'OK' button is highlighted with a red box and labeled 'b)'. The text above the dropdown says 'ダウンロード処理を開始する領域を選択してください' (Please select the area to start the download process).

(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。

The screenshot shows the 'PAN-DB URL Filtering' license page. The 'ダウンロードの状態' (Download status) is now '2018-02-07 22:36:19 PAN-DB download: Finished successfully: 再ダウンロード' (2018-02-07 22:36:19 PAN-DB download: Finished successfully: Re-download). The text 'Finished successfully' is highlighted with a red dashed box.

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。



- (2) 「今すぐチェック」をクリックします。

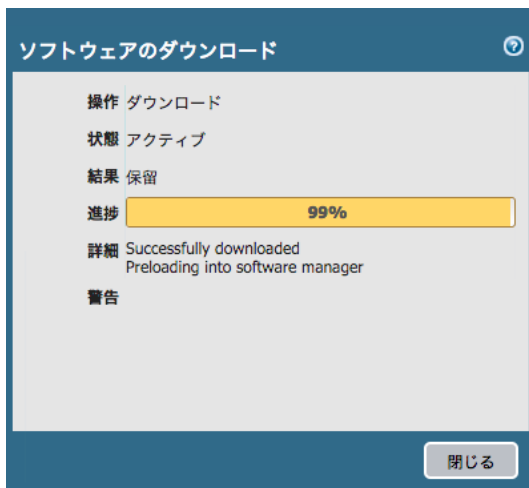


- (3) 現在リリースされている OS の一覧が表示されます。

- 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。



(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。

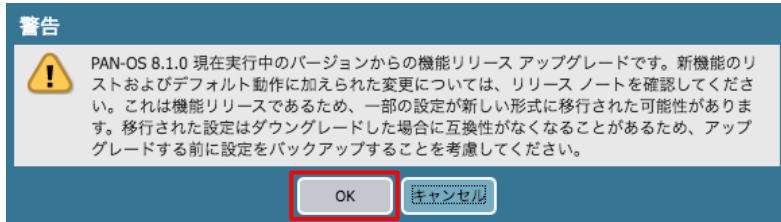


(5) 「インストール」をクリックします。

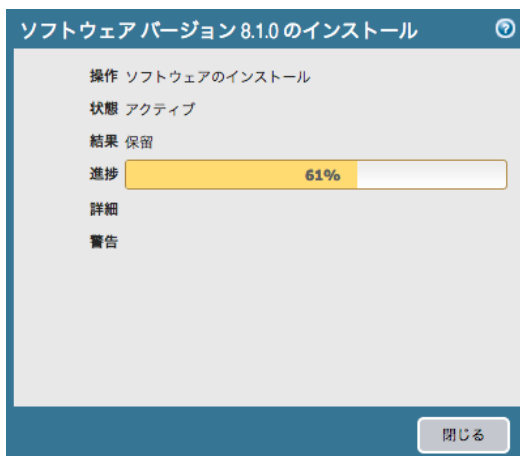


(6) 以下のような警告が出ます。

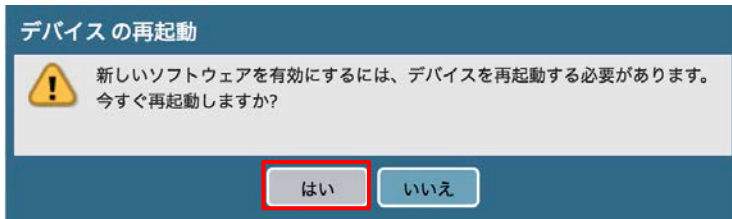
ここまでの設定では、バックアップを要するほどの設定はしていませんので、「OK」をクリックします。



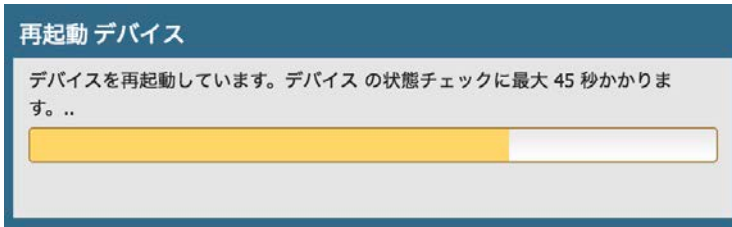
(7) インストールが開始されます。完了するまで待ちます。



(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。

The screenshot shows the Palo Alto Networks WebUI Dashboard. The "Dashboard" tab is selected and highlighted with a red box. The "一般的な情報" (General Information) panel is expanded, showing various system details. The "ソフトウェアバージョン" (Software Version) field is highlighted with a red box and labeled "b)". The "システムログ" (System Log) panel shows a list of events, including "Config installed" and "User admin logged in via Web from 192.168.55.1 using https". The "設定ログ" (Configuration Log) panel shows a list of configuration changes.

デバイス名	PA-VM
MGT IP アドレス	192.168.55.11
MGT ネットマスク	255.255.255.0
MGT デフォルト ゲートウェイ	192.168.55.2
MGT IPv6 アドレス	unknown
MGT IPv6 リンク ローカル アドレス	fe80::20c:29ff:fe88:b63d/64
MGT IPv6 デフォルト ゲートウェイ	
MGT MAC アドレス	00:0c:29:88:b6:3d
モデル	PA-VM
シリアル番号	01535100008994
CPU ID	ESX:E9060900FFFBAB1F
UUID	564D0A8E-7D8A-4A3C-64B3-1EFF2C88B63D
VM ライセンス	VM-50
VM モード	VMWare ESXi
ソフトウェアバージョン	8.1.0
GlobalProtect エージェント	0.0.0

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
admin	192.168.55.1	Web	03/24 17:28:29	00:00:00s

内容	時間
Autocommit job succeeded	03/24 17:28:31
Dnsproxy object:mgmt-obj was enabled.	03/24 17:28:29
KEYMGR sync all IPsec SA to Flow exit.	03/24 17:28:29
Config installed	03/24 17:28:29
KEYMGR sync all IPsec SA to Flow started.	03/24 17:28:29
User admin logged in via Web from 192.168.55.1 using https	03/24 17:28:29

コマンド	パス	管理者	時間
commit		admin	03/24 17:10:51
set	deviceconfig system	admin	03/24 17:10:40
set	deviceconfig system	admin	03/24 17:10:19
delete	deviceconfig system dns-setting dns-proxy-object	admin	03/24 17:10:18
delete	deviceconfig system dns-setting dns-proxy-object	admin	03/24 17:10:18
commit		admin	03/24 17:07:06
set	deviceconfig system type	admin	03/24 17:07:02
set	deviceconfig system	admin	03/24 17:06:57

4. ネットワーク設定

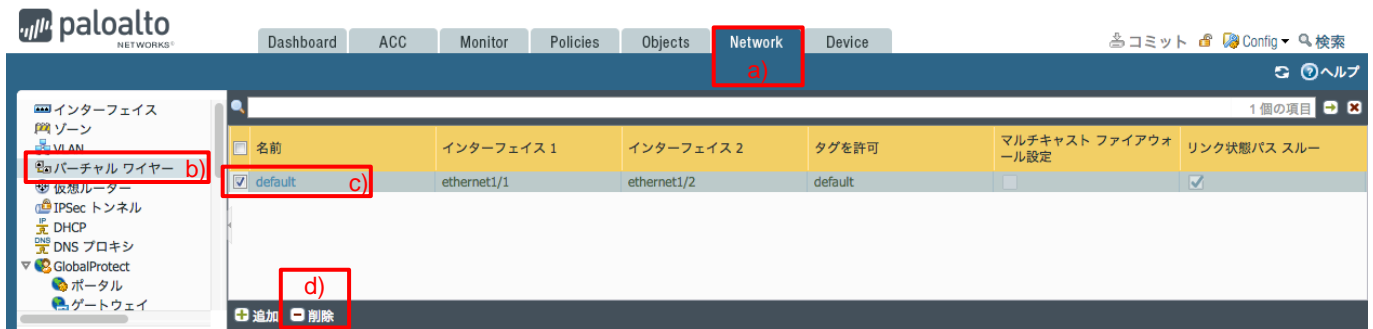
ゾーンやインターフェイス及びルーティングなどのネットワーク設定を行います。

4.1. Virtual Wire 設定の削除

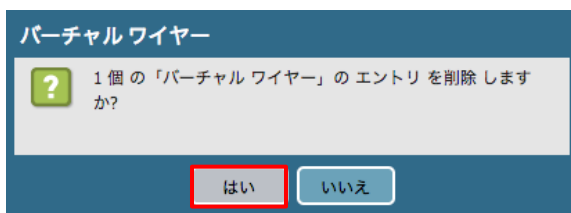
デフォルト状態で Virtual Wire の設定が存在しているかもしれません。

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



(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」 → b)「ゾーン」 → c)「追加」をクリックします。

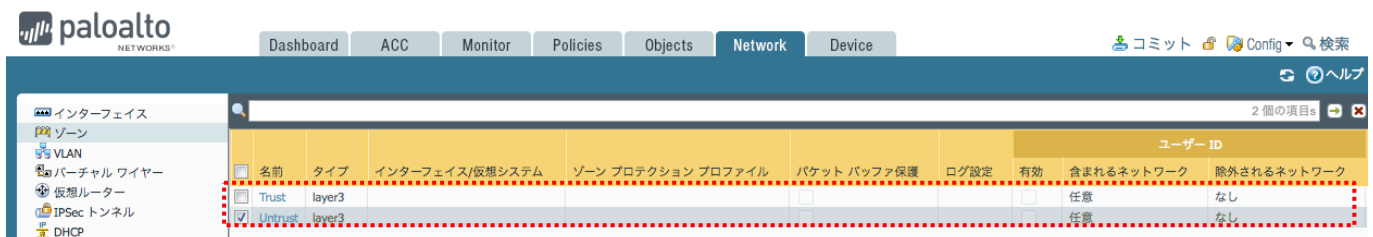


(2) 表示された画面で、a)名前に「Trust」、b)タイプで「レイヤー3」を選択して、b)「OK」をクリックします。



(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。



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。

(1) a)「Network」 → b)「インターフェイス」 → c)「ethernet1/1」をクリックします。



(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。



- (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

インターフェイス名 ethernet1/1
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 **a) IPv4** IPv6 詳細

タイプ スタティック PPPoE DHCP クライアント

IP
<input checked="" type="checkbox"/> 192.168.55.20/24 c)

b) 追加 削除 上へ 下へ

IP アドレス/ネットマスク (例: 192.168.2.254/24)

OK キャンセル

- (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

インターフェイス名 ethernet1/1
コメント
インターフェイスタイプ レイヤー 3
Netflow プロファイル None

設定 IPv4 IPv6 **a) 詳細**

リンク設定
リンク速度 auto リンク デュプレックス auto リンク状態 auto

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 **b)** None
MTU None

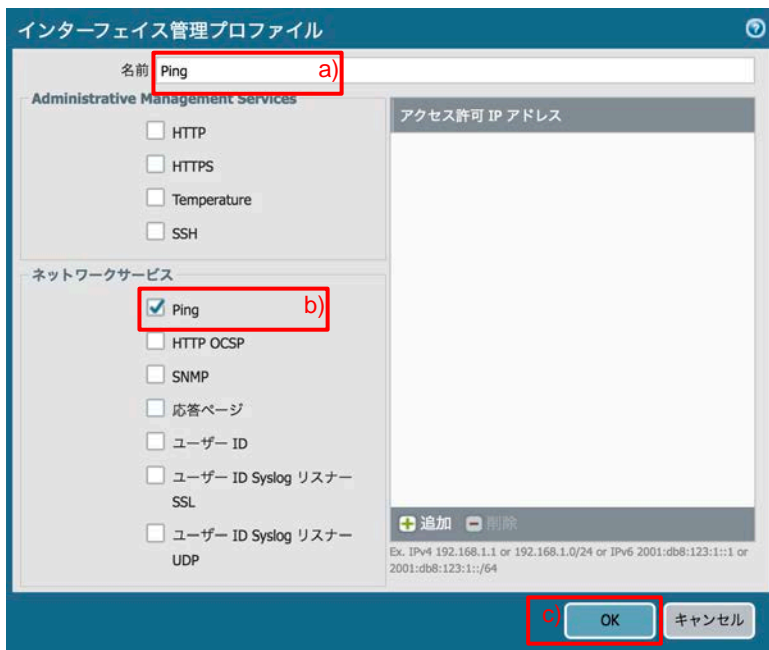
TCP MSS の調整 **c) 管理プロファイル**

IPv4 MSS 調整	40
IPv6 MSS 調整	60

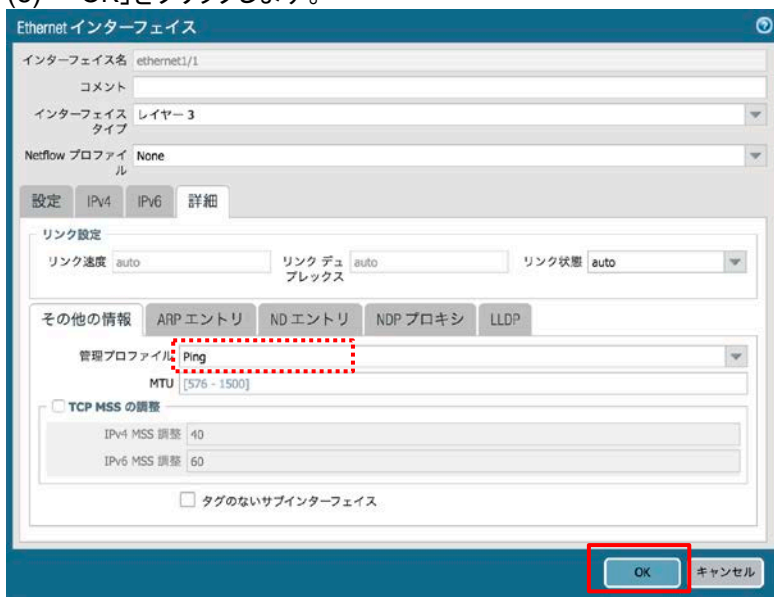
タグのないサブインターフェイス

OK キャンセル

- (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。



- (6) 「OK」をクリックします。



- (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」 → b)「仮想ルーター」 → c)「default」をクリックします。



(2) a)「スタティックルート」 → b)「追加」をクリックします。



- (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。

- (4) 「OK」をクリックします。

名前	宛先	インターフェイス	ネクスト ホップ		管理距離	メトリック	BFD	ルート テーブル
			タイプ	値				
default_route	0.0.0.0/0	ethernet1/1	ip-address	192.168.55.2	default	10	None	unicast

- (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。

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
ethernet1/1	Layer3	Ping	Link Up	192.168.55.20/24	default	Untagged	none	Untrust	
ethernet1/2	Layer3	Ping	Link Up	192.168.45.20/24	default	Untagged	none	Trust	

5. NAT

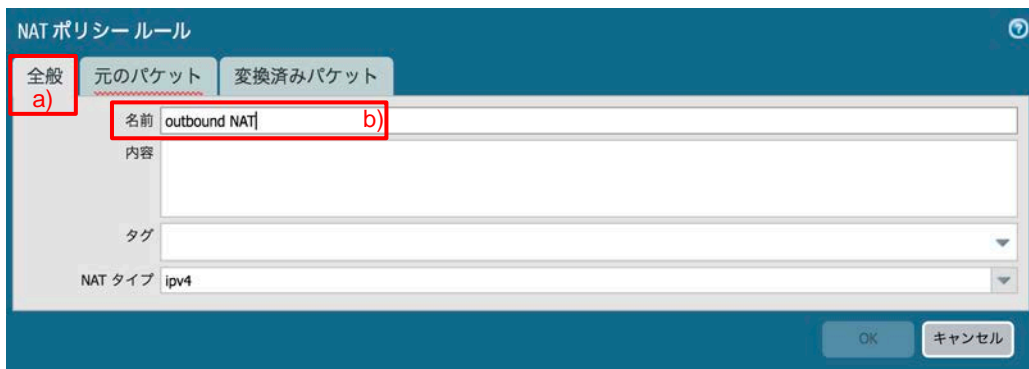
本ガイドでは、Trust ゾーンのサブネット:192.168.45.0/24 の端末から Untrust 方向(インターネット方向)へは、送信元アドレスを、ethernet1/1 に設定された IP アドレス:192.168.55.20 にアドレス変換して通信することになります。

その設定方法を以下に示します。

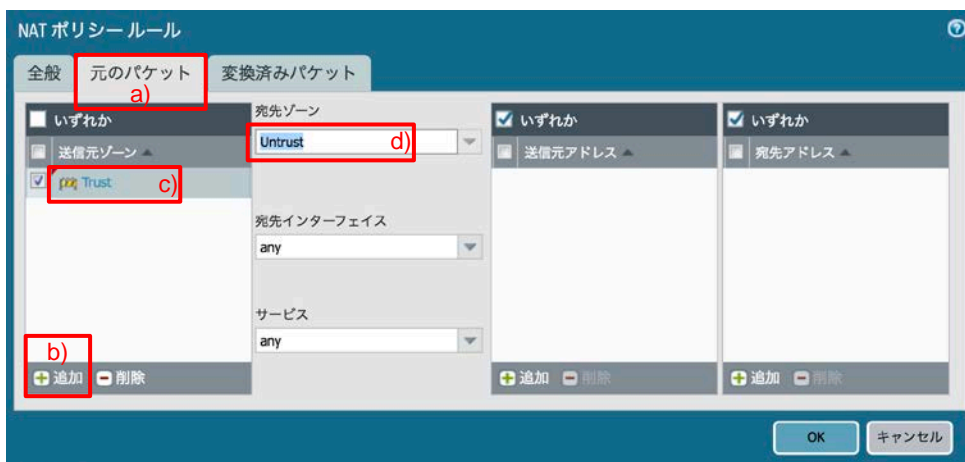
(1) a)「Policies」 → b)「NAT」 → c)「追加」をクリックします。



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



(3) a)「元の packets」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。



- (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 およびポート」、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。

(5) 以下は、NAT 設定後の状態です。

		元のパケット					変換済みパケット			
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	Trust	Untrust	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」 → b)「セキュリティ」で表示された画面の c)の部分です。

名前	タグ	タイプ	送信元				宛先		ルールの使用状況			アプリケーション
			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	ヒット数	最後のヒット	最初のヒット	
1 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	0	-	-	any
2 interzone-default	none	interzone	any	any	any	any	any	any	0	-	-	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。

名前	タグ	タイプ	送信元				宛先		アプリケーション	サービス	アクション	プロ
1 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	名前			
2 interzone-default	none	interzone	any	any	any	any	any	any	タグ			

- 名前
- タグ
- タイプ
- 送信元 ゾーン
- 送信元 アドレス
- 送信元 ユーザー
- 送信元 HIP プロファイル
- 宛先 ゾーン
- 宛先 アドレス
- ルールの使用状況 ヒット数
- ルールの使用状況 最後のヒット
- ルールの使用状況 最初のヒット
- 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。

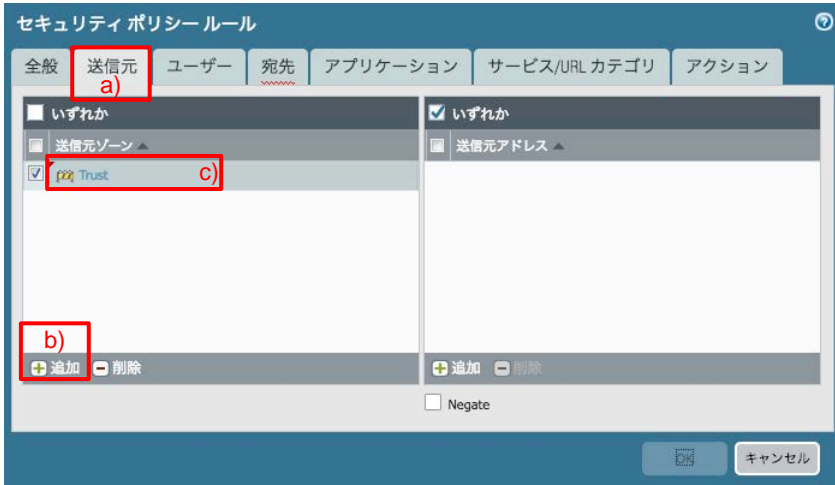
(1) a)「Policies」 → b)「セキュリティ」 → c)「追加」をクリックします。



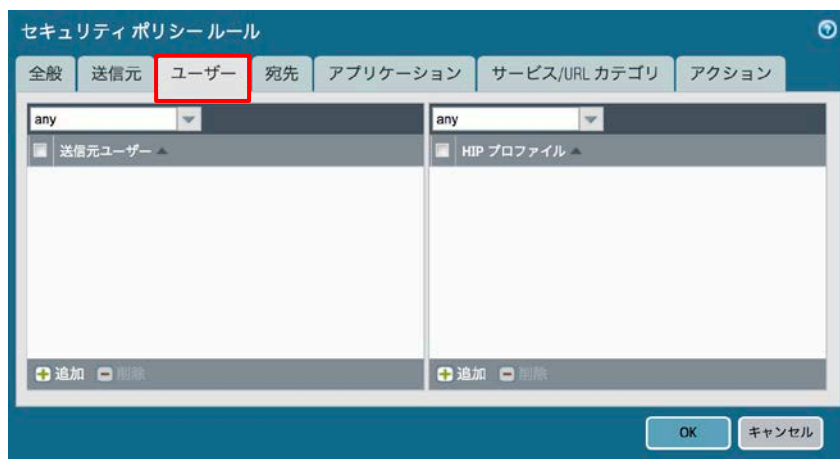
(2) a)「全般」タブで、b)名前に「allow outbound (任意)」と入力します。



(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。



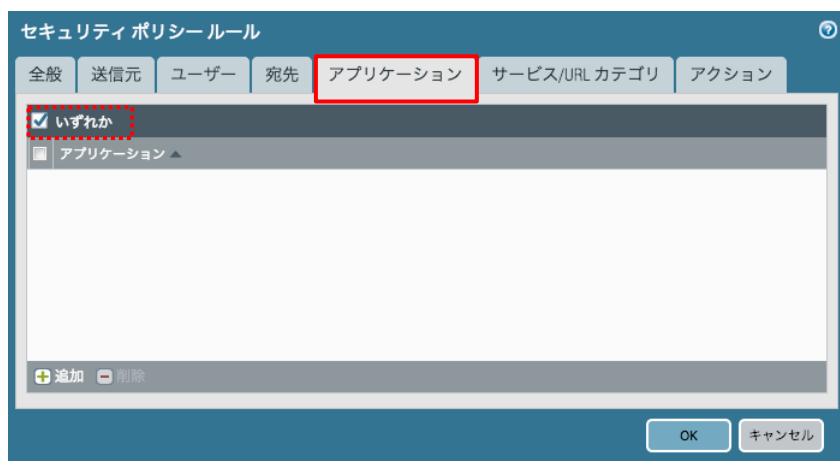
- (4) 「ユーザー」タブは、デフォルトのまま「any」とします。
(※User-ID 連携を行った場合に、ユーザ名でポリシー制御を行う場合は、このタブで設定します。)



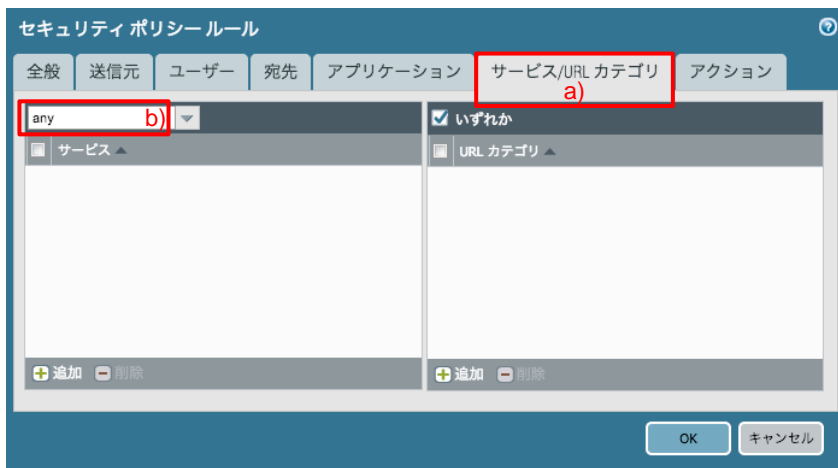
- (5) a)「宛先」タブで、b)「追加」をクリックし、c)「Untrust」を選択します。



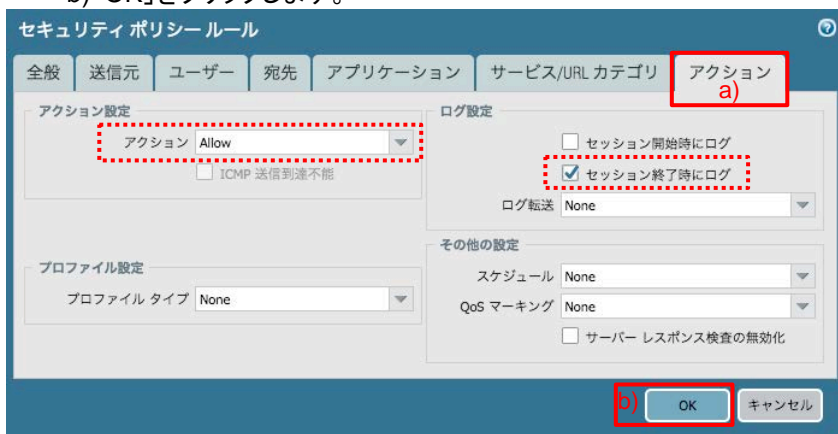
- (6) 「アプリケーション」タブは、デフォルトのまま「いずれか」とします。



(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。



(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。



(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	タグ	タイプ	送信元				宛先				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
			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							
1 allow outbound	none	universal	Trust	any	any	any	Untrust	any	any	any	any	許可	none		
2 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	許可	none	none	
3 interzone-default	none	interzone	any	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 サイトへ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。

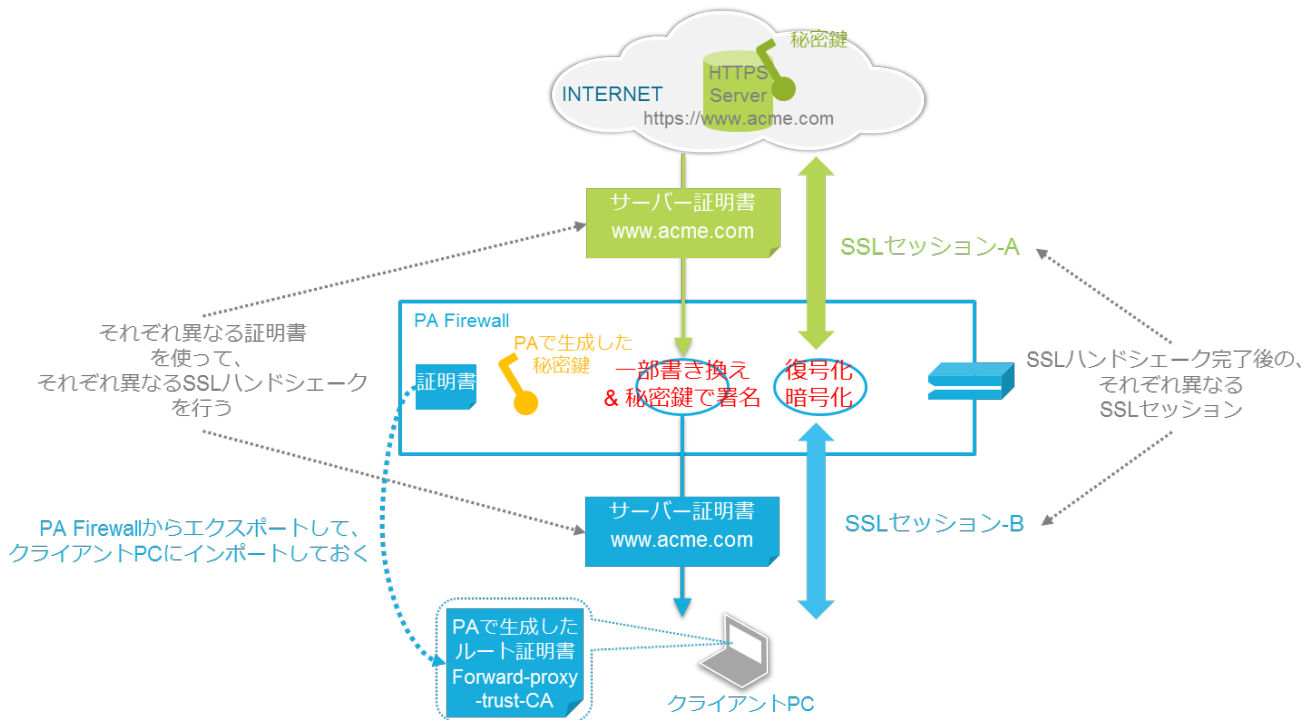


7. SSL/TLS 復号化の設定

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。

- ① (SSL セッション確立前の) SSL ハンドシェイクの段階で、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 ハンドシェイクで、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 ハンドシェイクが行われる。
- ⑥ SSL ハンドシェイクが完了すると、「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

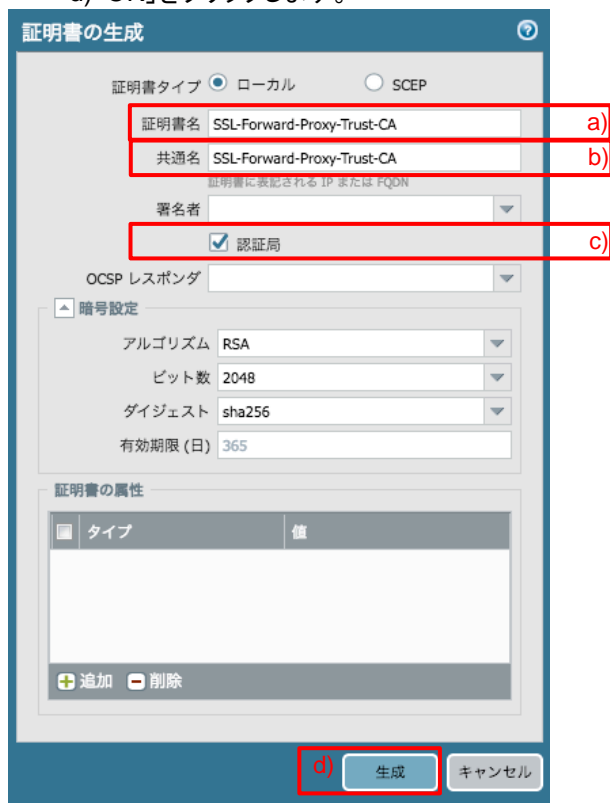
PA Firewall がインターネットに存在する Web サイトのサーバー証明書を受け取り、それを書き換えてクライアントに送り出すためには、PA Firewall 内に認証局の秘密鍵が必要です。

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。)

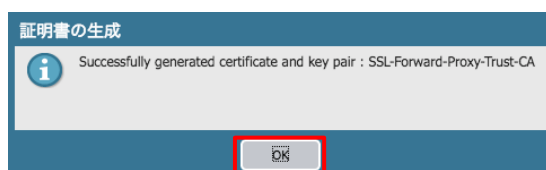
(1) a)「Device」 → 「証明書の管理」の下の b)「証明書」 → c)「生成」をクリックします。



(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。



(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 ハンドシェイクを行う、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。



(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。



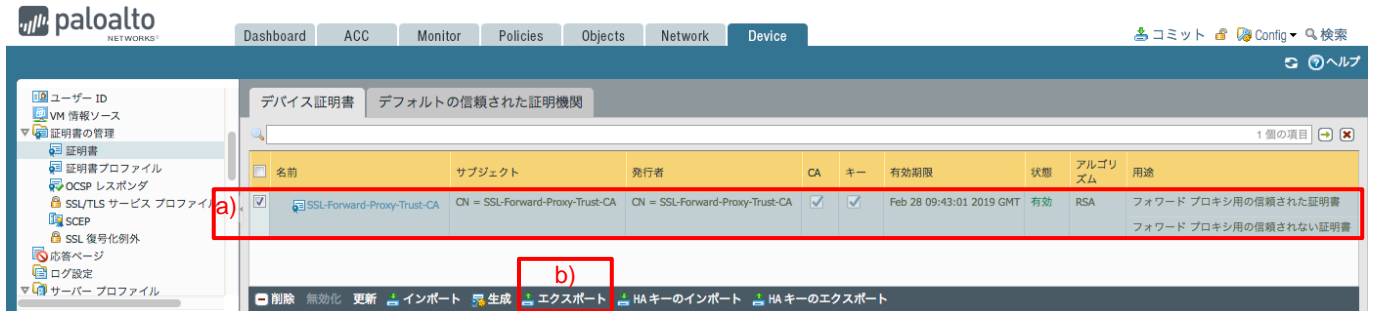
7.3. 証明書のエクスポートとインポート

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 へインポートします。

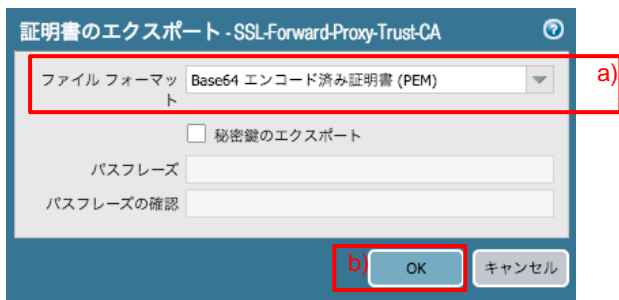
7.3.1. 証明書のエクスポート

「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 へインポートします。)

(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。



(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。



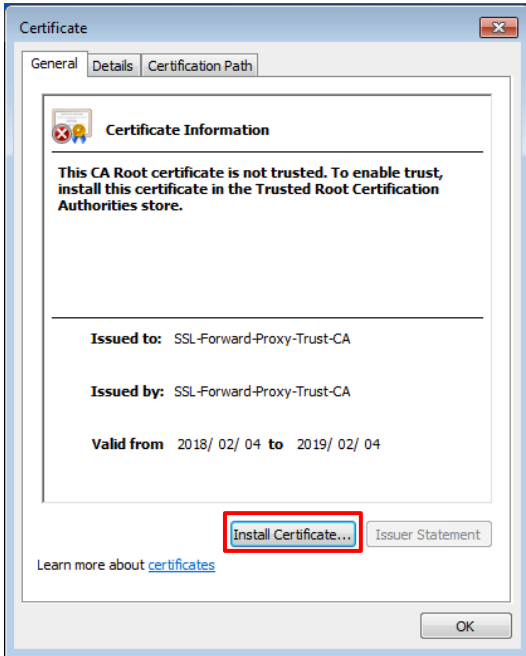
(3) エクスポートされたルート証明書を、一時的にコンソール PC へ保存しておきます。

7.3.2. クライアント PC ヘルート証明書をインポート

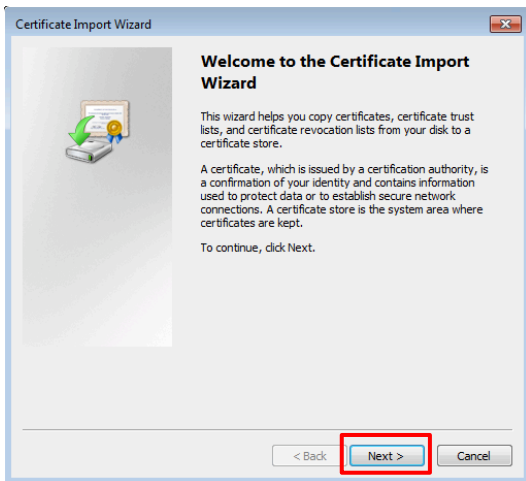
PA Firewall からエクスポートしたルート証明書を、Trust ゾーンのクライアント PC へインポートします。

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。

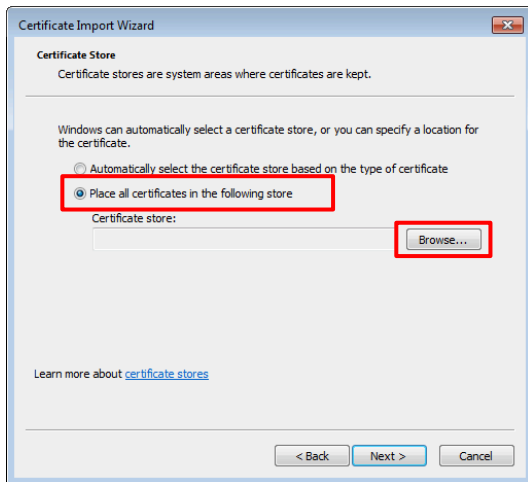
- (1) PA Firewall からエクスポートしたルート証明書を、クライアント PC(例:Windows7)へコピーします。
- (2) そのファイルをダブルクリックして表示された画面で、「Install Certificate / 証明書のインストール」をクリックします。



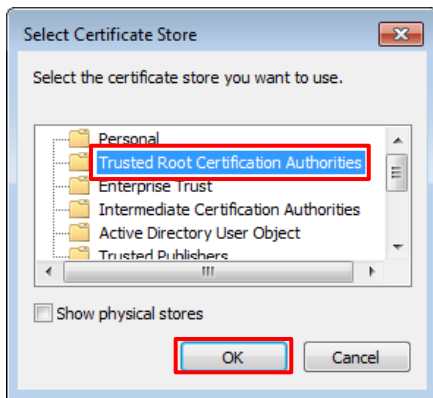
- (3) 「Next / 次へ」をクリックします。



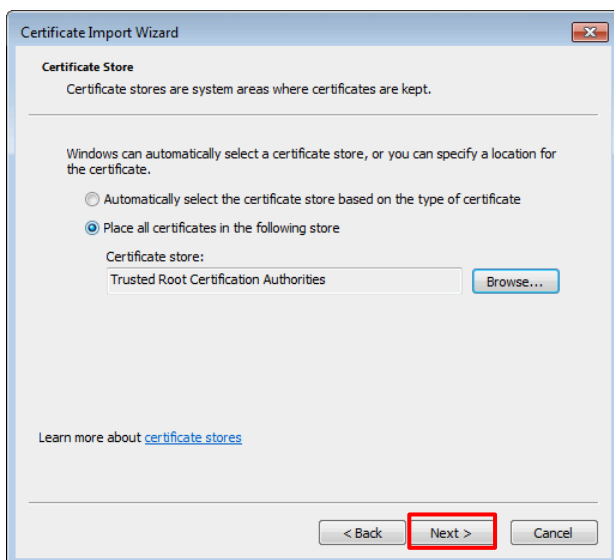
- (4) 「Place all certificate in the following store / 証明書を全て次のストアに配置する」を選択して、「Browse.../参照」をクリックします。



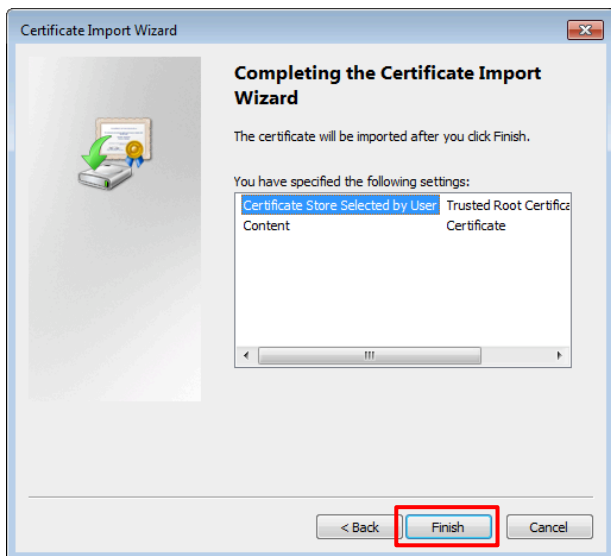
- (5) 「Trusted Root Certification Authorities / 信頼されたルート証明機関」を選択して、「OK」をクリックします。



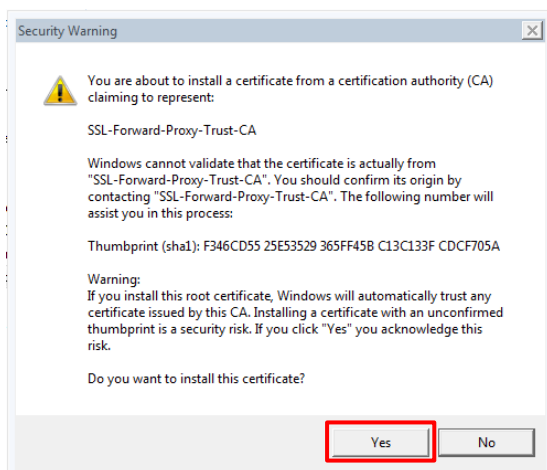
- (6) 「Next / 次へ」をクリックします。



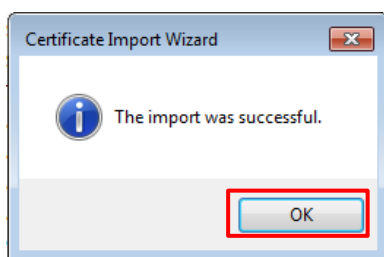
(7) Finish をクリックします。



(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

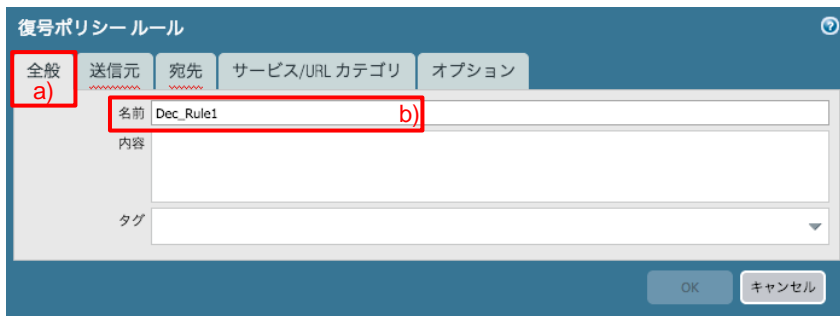
SSL 復号化を行うには、どのような条件(例:送信元や宛先)の場合に復号するのか、という復号ポリシーの設定も必要です。

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」 → b)「復号」 → c)「追加」をクリックします。



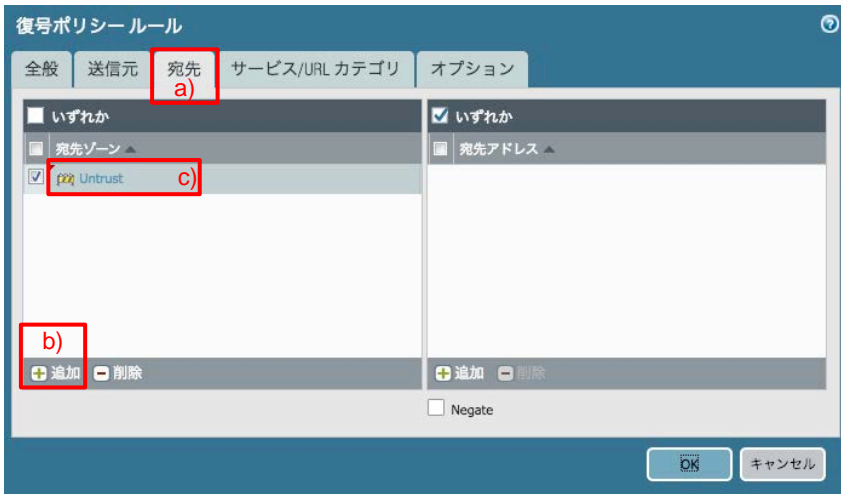
(2) a)「全般」タブで、b)名前に「Dec_Rule1 (任意)」と入力します。



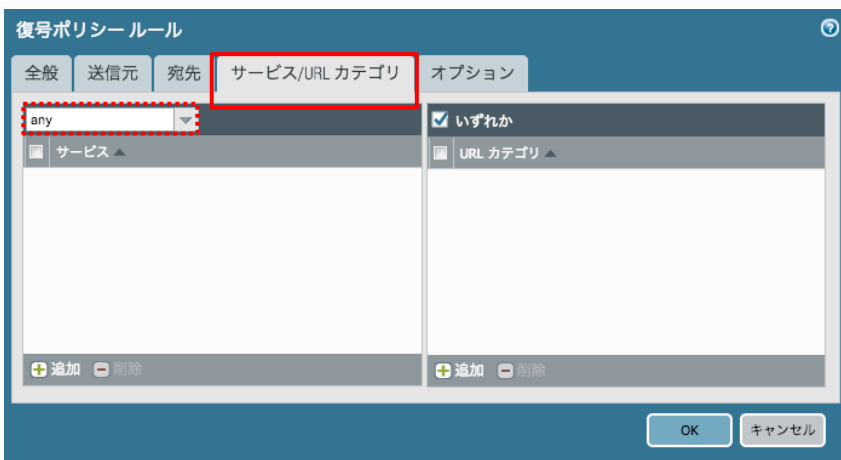
(3) a)「送信元」タブで、b)「追加」をクリックし、c)「Trust」を選択します。



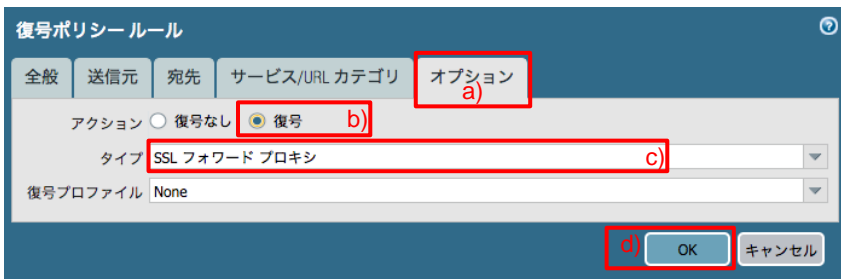
(4) a)「宛先」タブで、b)「追加」をクリックし、c)「Untrust」を選択します。



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



(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。



(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

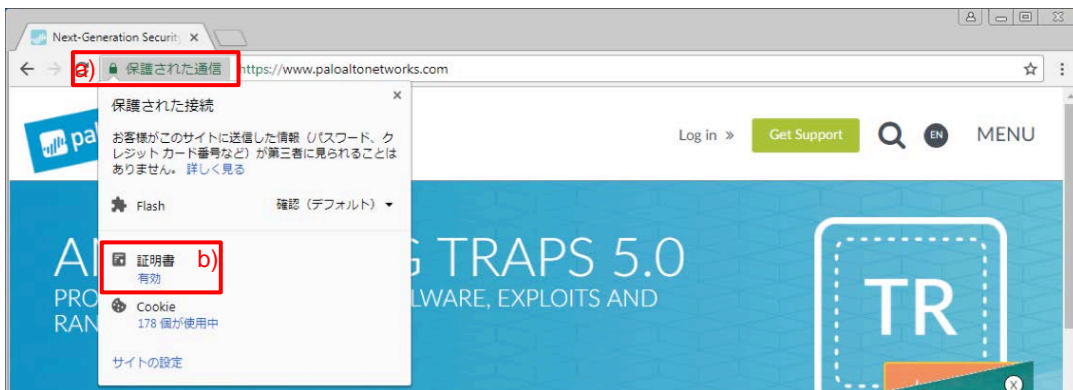
7.5.1. 「信頼された証明書」を持つサイトへの通信確認

一般的なインターネット上の HTTPS サイトへ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。

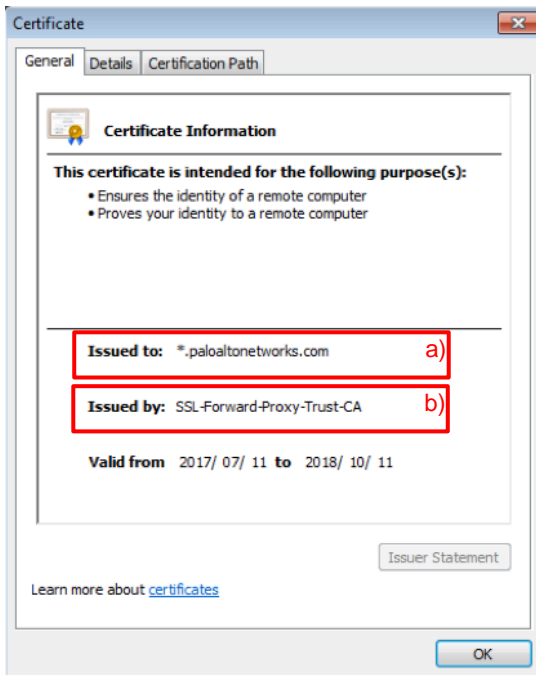
Chrome ブラウザの場合： Google が提供するサイト”以外”の HTTPS サイトで確認してください。
Chrome が Google 提供サイトへアクセスする場合には、初動として QUIC(UDP/443)を利用する機会が多く、v8.1 においても PA Firewall は QUIC の復号化をサポートしていないため、QUIC が通過する現段階では、復号化が動作しません。
後に QUIC を拒否する設定に変更します。

(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: <https://www.paloaltonetworks.com>) へアクセスします。

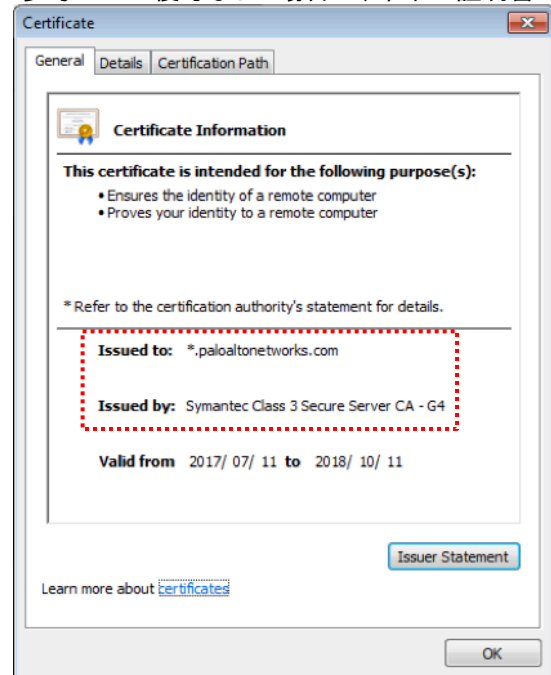
(2) Chrome ブラウザの a)「保護された通信」 → b)証明書の下の「有効」をクリックします。



(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




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 に渡しているため、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。

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。



	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
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		66.151.25.23	443	ssl	allow	allow outbound
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		66.151.25.23	443	ssl	allow	allow outbound
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		54.186.44.170	443	ssl	allow	allow outbound
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		54.186.44.170	443	ssl	allow	allow outbound
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		104.237.191.1	443	web-browsing	allow	allow outbound
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		13.33.9.100	443	ssl	allow	allow outbound
	03/25 11:20:52	end	Trust	Untrust	192.168.45.32		13.33.9.100	443	ssl	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。



PCAP	受信日時 ▲	タイプ	アプリケーション	アクション	ルール	バイト	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 outbound	8521		computer-and-internet-info			

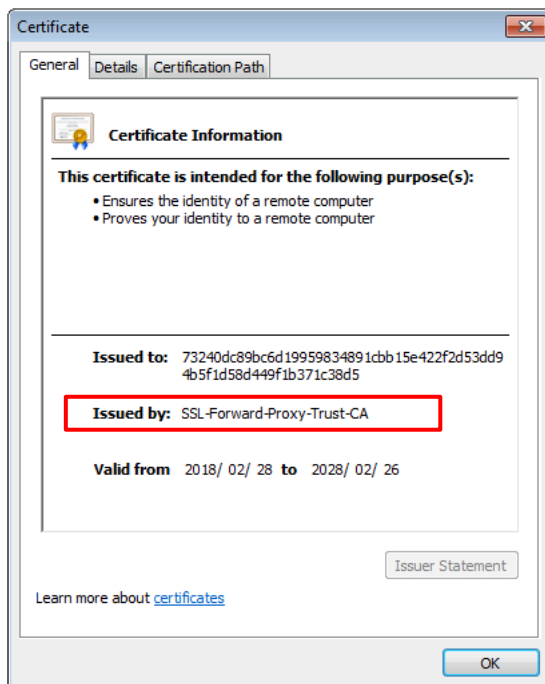
7.5.3. 「信頼されない証明書」を持つサイトへの通信確認

「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。

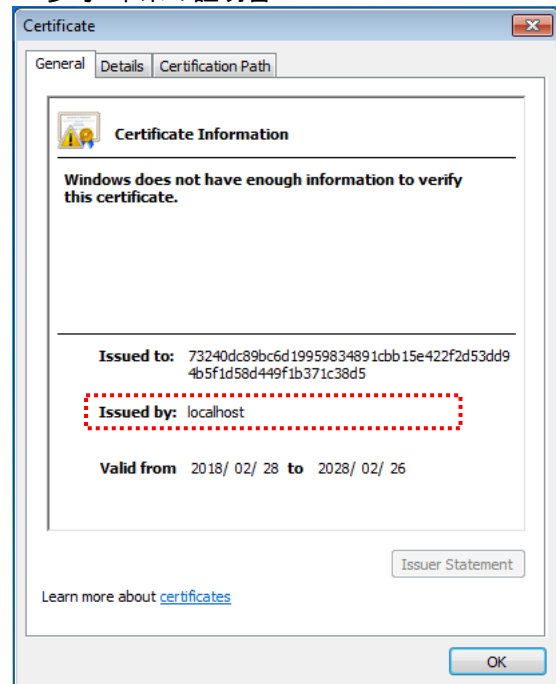
- (1) Trust ゾーン: 192.168.45.0/24 のクライアント PC の Web ブラウザ(例:Chrome)で、PA Firewall のマネージメントインターフェイス (<https://192.168.55.11>) へアクセスします。
- (2) Chrome の a)「保護されていません」 → b)証明書の下の「無効」をクリックします。



- (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



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ずに、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」 → b)「証明書」 → c)「生成」をクリックします。



(2) 以下の通り設定し、仮の認証局を生成します。

The screenshot shows the '証明書生成' (Certificate Generation) configuration window. The 'ローカル' (Local) radio button is selected. The '証明書名' (Certificate Name) and '共通名' (Common Name) fields are both set to 'dummy-CA'. The '署名者' (Signer) dropdown is set to '認証局' (CA), which is checked. The '暗号設定' (Encryption Settings) section shows 'アルゴリズム' (Algorithm) set to RSA, 'ビット数' (Bit Length) set to 2048, 'ダイジェスト' (Digest) set to sha256, and '有効期限(日)' (Validity Period) set to 365. The '生成' (Generate) button is highlighted with a red box.

証明書タイプ ローカル SCEP

証明書名 dummy-CA(任意)

共通名 dummy-CA(任意)

署名者 認証局 認証局にチェック

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	値
-----	---

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」 → b)「証明書」 → 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

証明書タイプ ローカル SCEP

証明書名 dummy-cert01(任意)

共通名 192.168.55.11

署名者 dummy-CA を選択

認証局

OCSF レスポンダ

暗号設定

アルゴリズム

ビット数


ダイジェスト

有効期限 (日)

タイプ	値
<input checked="" type="checkbox"/> IP	192.168.55.11

(※ ↑「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)  アイコンをクリックします。



(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

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 バナーの確認を管理者に強制

SSL/TLS サービス プロファイル None a)

タイムゾーン 新規 SSL/TLS サービス プロファイル b)

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

最小バージョン TLSv1.0

最大バージョン 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

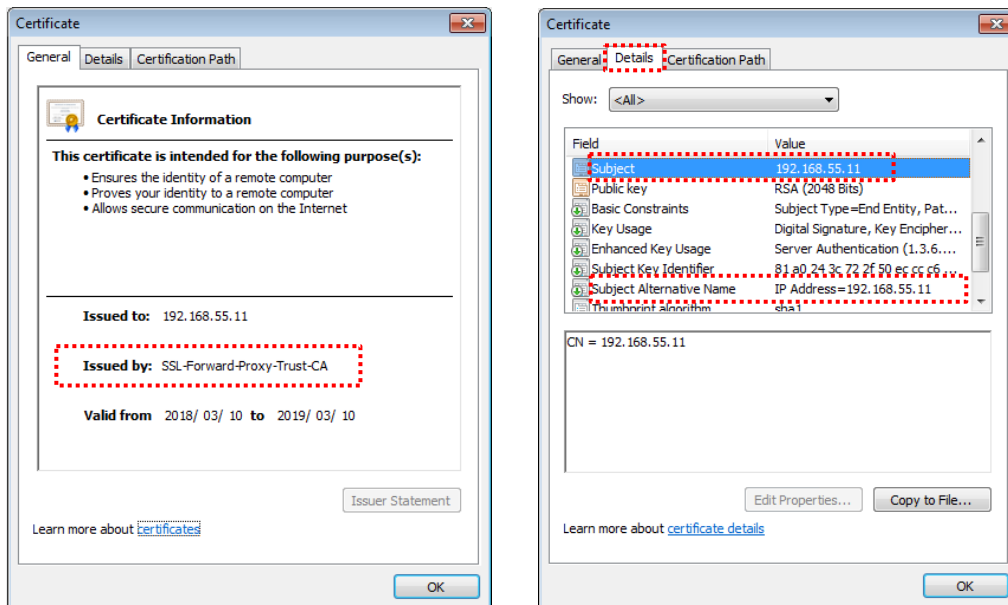
- (1) クライアント PC の Web ブラウザから PA Firewall のマネージメントインターフェイス (<https://192.168.55.11>) へアクセスします。
- (2) 「保護された通信」として扱われてしまいます。

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」であるにもかかわらず、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。

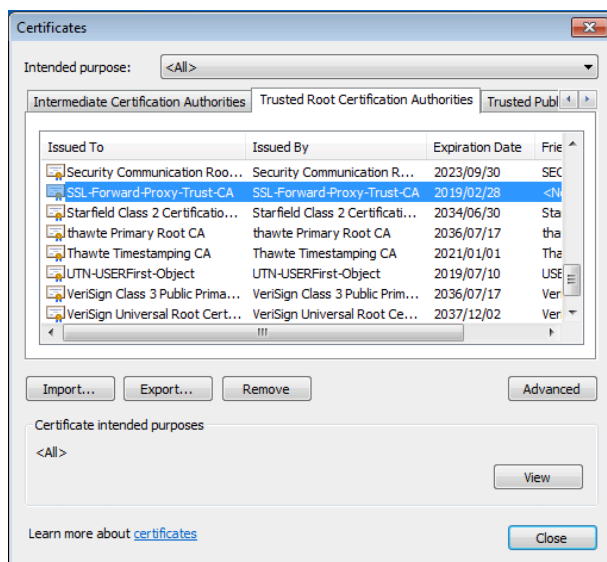
- ① サーバー証明書の署名が、クライアント PC 内の「Trusted Root Certification Authorities/信頼されたルート証明機関」に存在する認証局によって署名されていること。(←Windows の例。他 OS にも類似の仕組みが存在する。)
- ② Common Name が一致すること。(Firefox, IE11)
- ③ SAN が一致すること。(Firefox, Chrome)

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。



次のセクションで、この現象を回避する設定を行います。

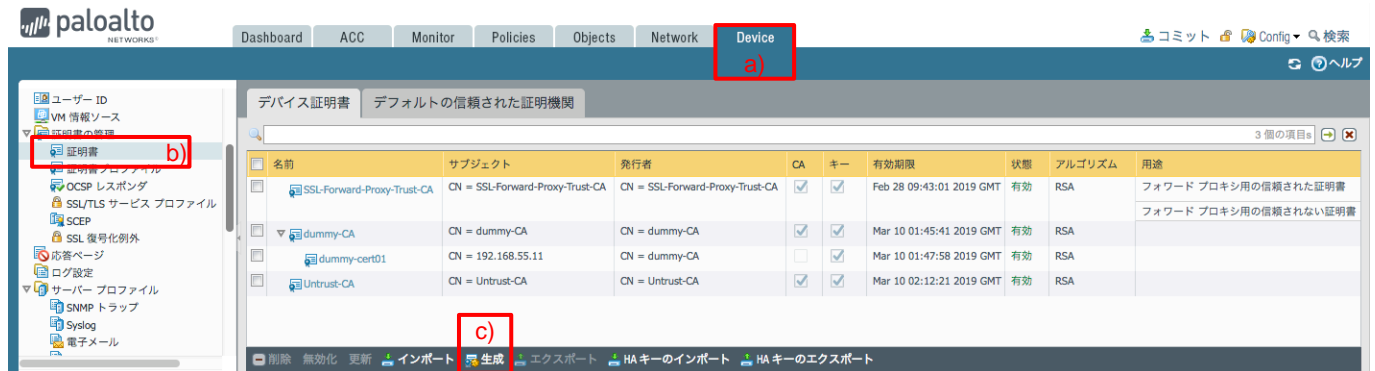
7.6.4. 「信頼されない証明書」用の認証局の生成

「信頼されない証明書」を持つサイトへクライアント 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。

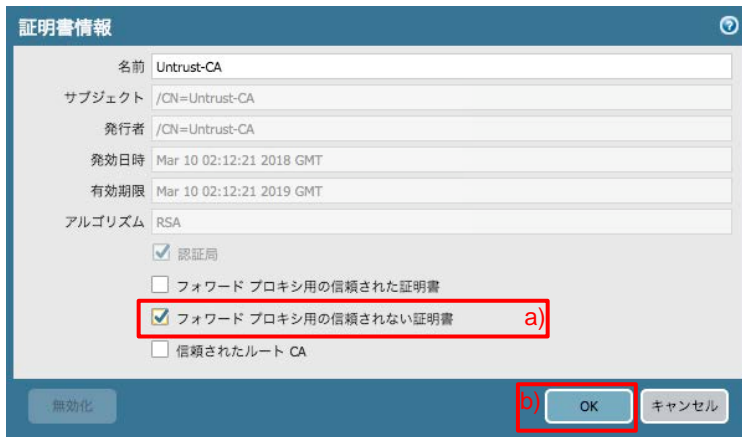
(1) a)「Device」 → b)「証明書」 → c)「生成」をクリックします。



(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。

The screenshot shows the '証明書の生成' (Certificate Generation) form. The form is set to 'ローカル' (Local) type. The '証明書名' (Certificate Name) and '共通名' (Common Name) fields are both set to 'Untrust-CA', with red boxes and labels 'Untrust-CA(任意)' pointing to each. The '署名者' (Signer) dropdown is set to '認証局' (CA), with a red box and label '認証局にチェック' pointing to the selection. The '暗号設定' (Encryption Settings) section shows 'アルゴリズム' (Algorithm) set to 'RSA', 'ビット数' (Bit Length) set to '2048', 'ダイジェスト' (Digest) set to 'sha256', and '有効期限 (日)' (Validity Period) set to '365'. The '生成' (Generate) button is highlighted with a red box.

- (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。



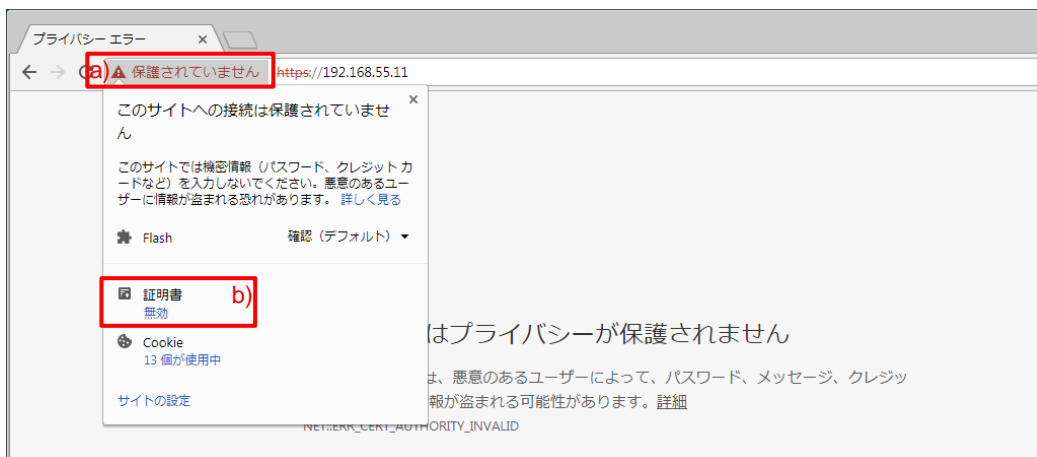
- (4) 以下のように、「SSL-Forward-Proxy-Trust-CA」の用途は「フォワードプロキシ用の信頼された証明書」だけになり、「Untrust-CA」の用途が、「フォワードプロキシ用の信頼されない証明書」になります。

名前	サブジェクト	発行者	CA	キー	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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 10 01:45:41 2019 GMT	有効	RSA	
dummy-cert01	CN = 192.168.55.11	CN = dummy-CA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 10 01:47:58 2019 GMT	有効	RSA	
Untrust-CA	CN = Untrust-CA	CN = Untrust-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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

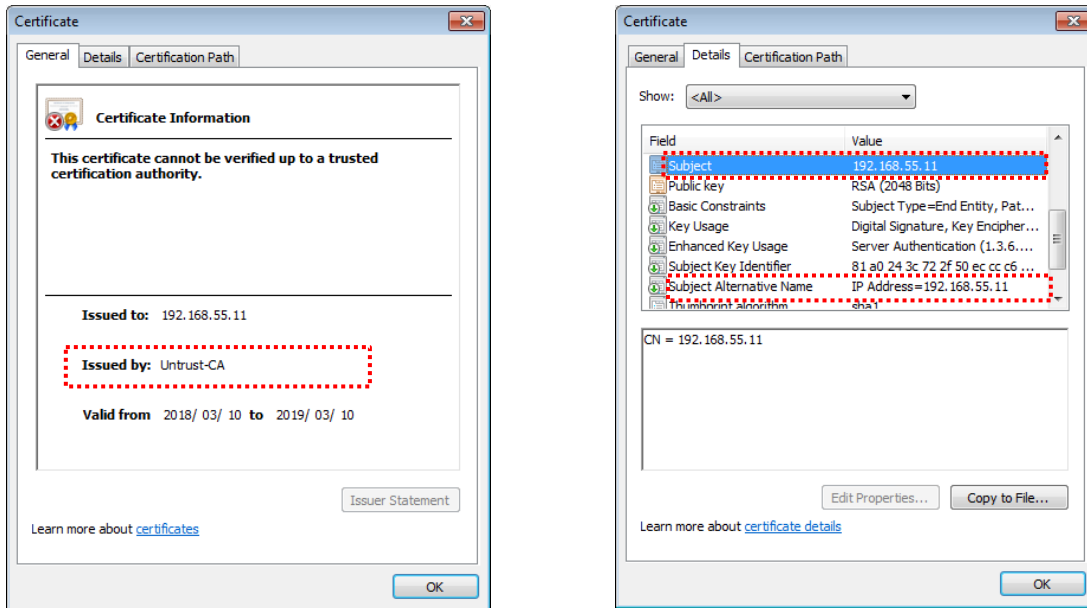
- (1) クライアント PC の Web ブラウザから PA Firewall のマネージメントインターフェイス (<https://192.168.55.11>) へアクセスします。
- (2) 今度は、「保護されていません」という結果になります。
 a)「保護されていません」 → b)証明書の下の「無効」をクリックします。



(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。



- Trust ゾーンの利用者に、「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

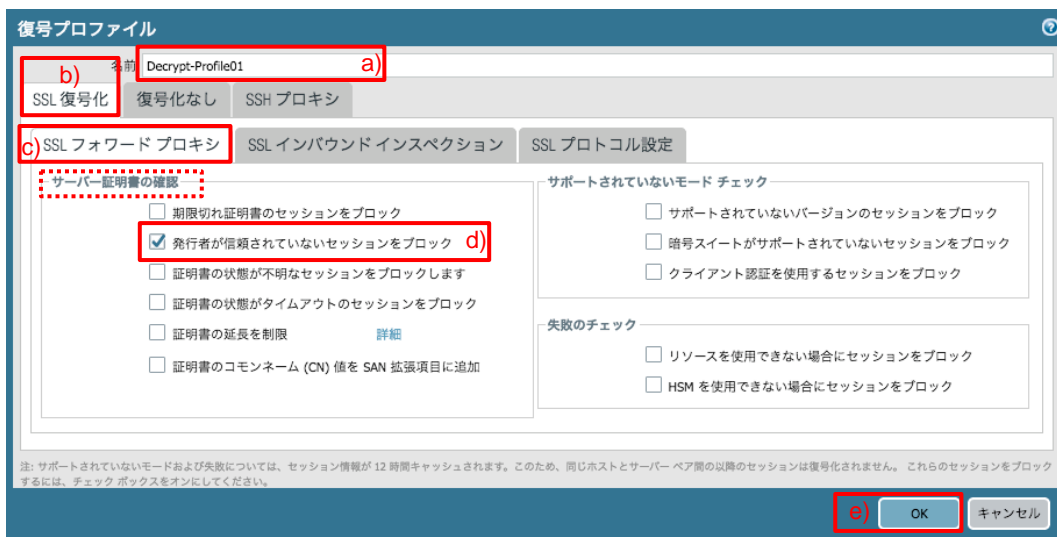
信頼された認証局から発行されたサーバー証明書を持たないサイトとの通信は、ブロックする設定が可能です。

7.7.1. 設定

(1) a)「Objects」 → 「復号」の下の b)「復号プロファイル」 → c)「追加」をクリックします。



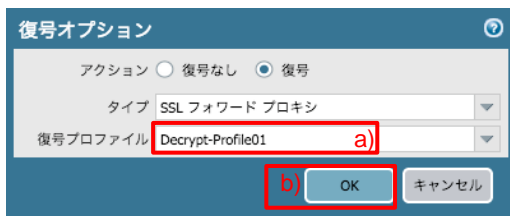
(2) a) 名前に「Decrypt_Profile01 (任意)」と入力します。
 b)「SSL 復号化」タブ → c)「SSL フォワードプロキシ」タブの、「サーバー証明書の確認」内にある d)「発行者が信頼されていないセッションをブロック」にチェックをいれます。e)「OK」をクリックします。



(3) a)「Policies」 → 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。



(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。

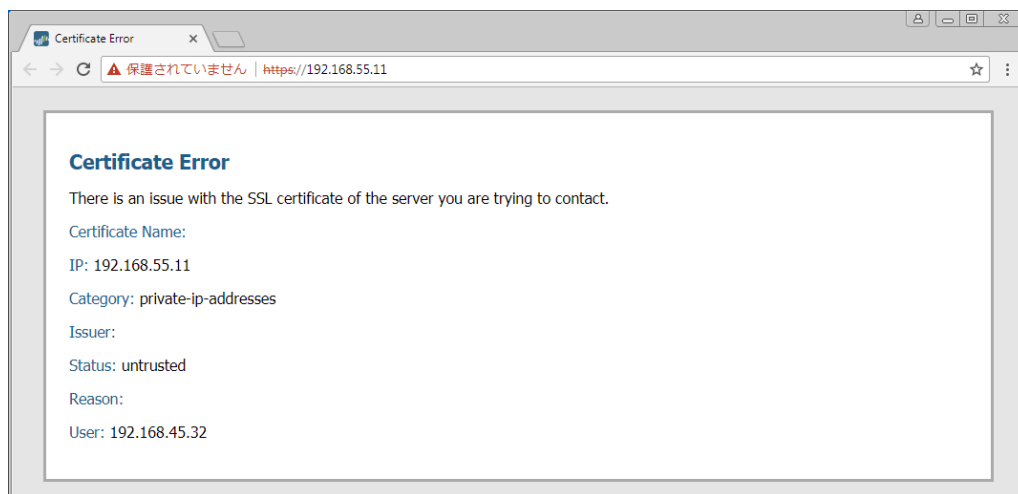


(5) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

7.7.2. 動作確認

(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、PA Firewall のマネージメントインターフェイス (<https://192.168.55.11>) へアクセスします。

(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。



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」 → b)「証明書」 → c)「デフォルトの信頼された証明機関」で確認できます。

The screenshot shows the Palo Alto Networks management console. The 'Device' tab is selected, and the 'Certificates' section is highlighted with a red box labeled 'b)'. The 'Default Trusted Certificate Authorities' section is highlighted with a red box labeled 'c)'. A table of certificate authorities is visible, including GeoTrust, GlobalSign, and Go Daddy.

名前	サブジェクト	発行者	有効期限	状態
GeoTrust_Primary_Certification_Authority - G2	GeoTrust Primary Certification Authority - G2	GeoTrust Primary Certification Authority - G2	Jan 18 23:59:59 2038 GMT	有効
GeoTrust_Primary_Certification_Authority - G3	GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Authority - G3	Dec 1 23:59:59 2037 GMT	有効
GeoTrust_Universal_CA	GeoTrust Universal CA	GeoTrust Universal CA	Mar 4 05:00:00 2029 GMT	有効
GeoTrust_Universal_CA_2	GeoTrust Universal CA 2	GeoTrust Universal CA 2	Mar 4 05:00:00 2029 GMT	有効
GlobalSign b	GlobalSign	GlobalSign	Jan 19 03:14:07 2038 GMT	有効
GlobalSign c	GlobalSign	GlobalSign	Jan 19 03:14:07 2038 GMT	有効
GlobalSign_Root_CA	GlobalSign Root CA	GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	有効
GlobalSign_Root_CA_-_R2	GlobalSign	GlobalSign	Dec 15 08:00:00 2021 GMT	有効
GlobalSign_Root_CA_-_R3	GlobalSign	GlobalSign	Mar 18 10:00:00 2029 GMT	有効
Global_Chambersign_Root_-_2008	Global Chambersign Root - 2008	Global Chambersign Root - 2008	Jul 31 12:31:40 2038 GMT	有効
Go_Daddy_Root_Certificate_Authority_-_G2	Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	有効
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
Mallinc Academic and Research	Mallinc Academic and Research	Mallinc Academic and Research	Dec 1 12:40:00 2021 GMT	有効

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。

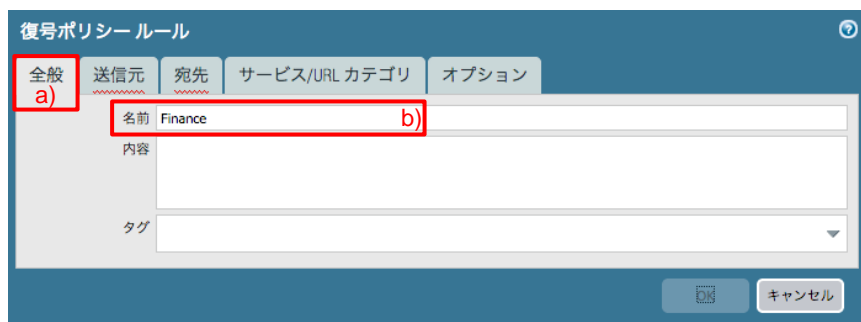
ここでは、「ユーザーのプライバシー保護の観点から、インターネットバンキングなどの金融系の復号化は行わない」という要件を想定し、その設定を行います。

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

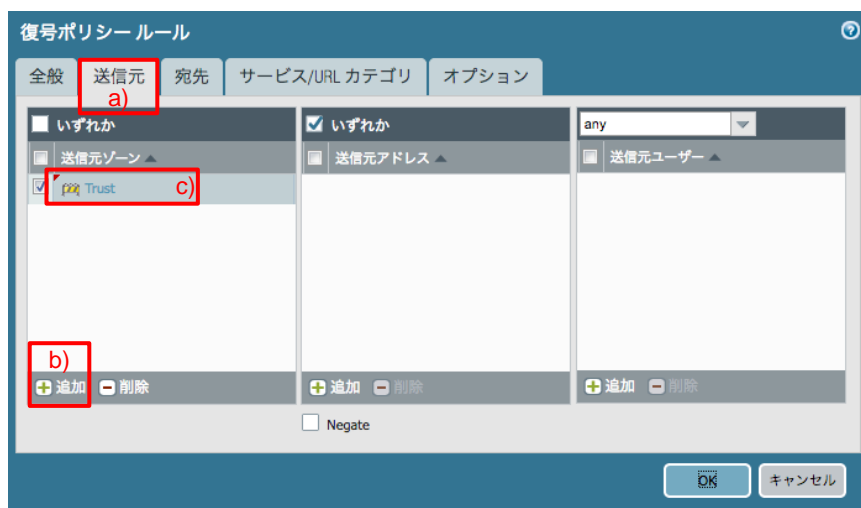
(1) a)「Policies」 → b)「復号」 → c)「追加」をクリックします。



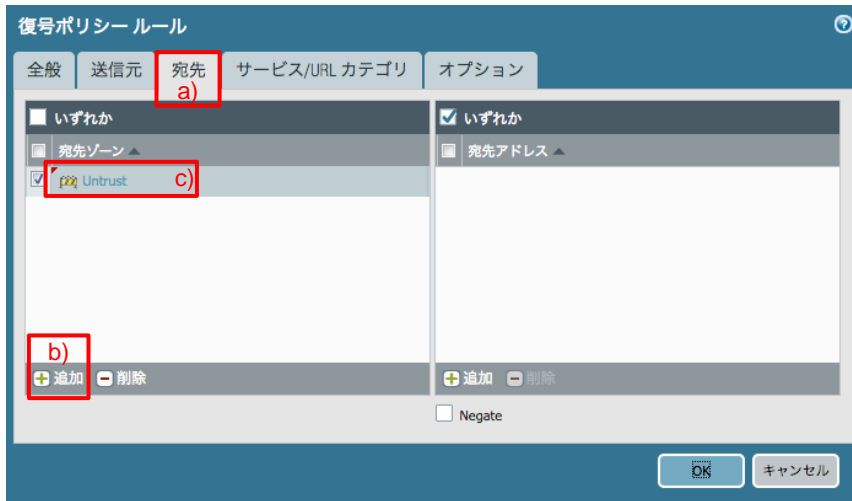
(2) a)「全般」タブで、b)名前に「Finance (任意)」と入力します。



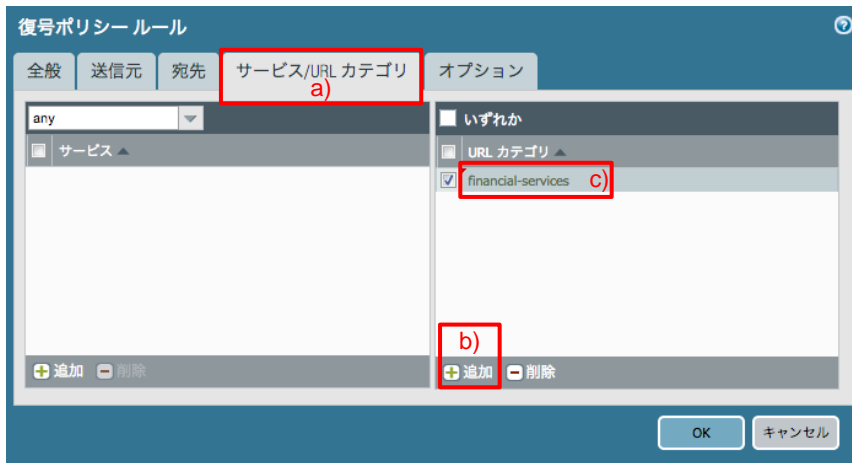
(3) a)「送信元」タブで、b)「追加」をクリックし、c)「Trust」を選択します。



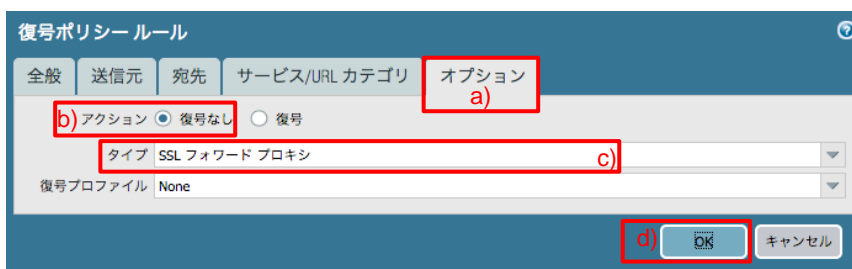
(4) a)「宛先」タブで、b)「追加」をクリックし、c)「Untrust」を選択します。



(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。)



(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。



(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。

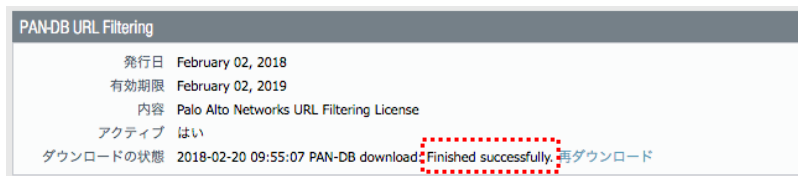


(8) 「Finance」が上へ移動した状態です。



(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。)



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。

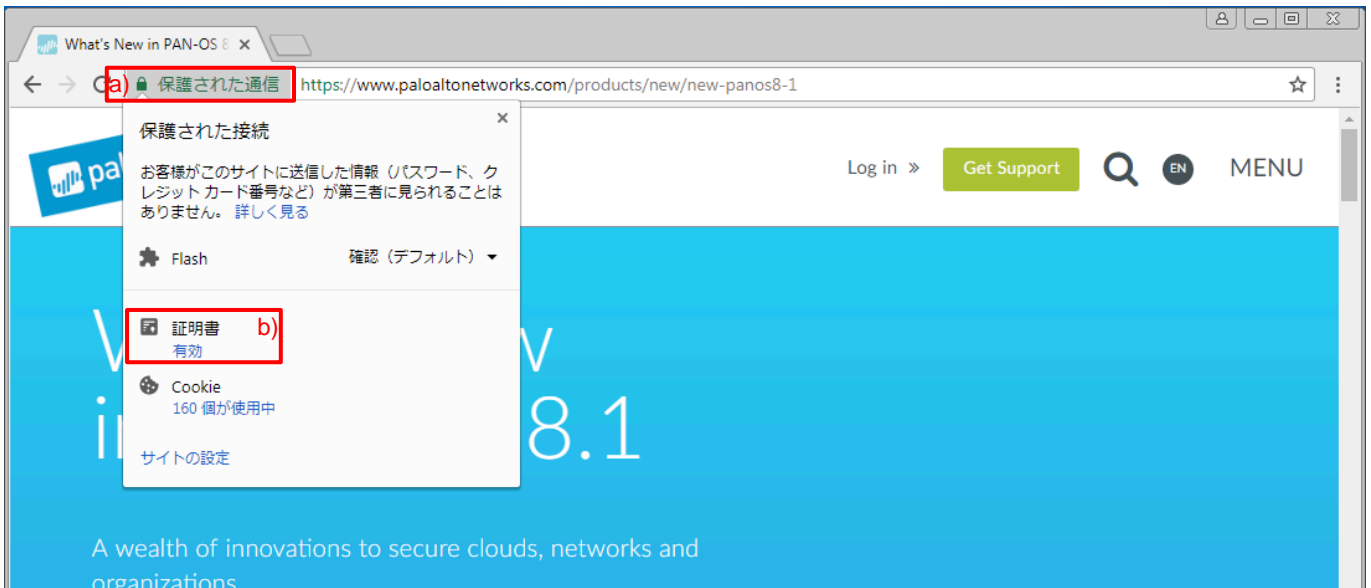


(2) Issued by / 発行者が、PA Firewall で生成した認証局(SSL-Forward-Proxy-Trust-CA)ではない(=復号化されていない)ことがわかります。

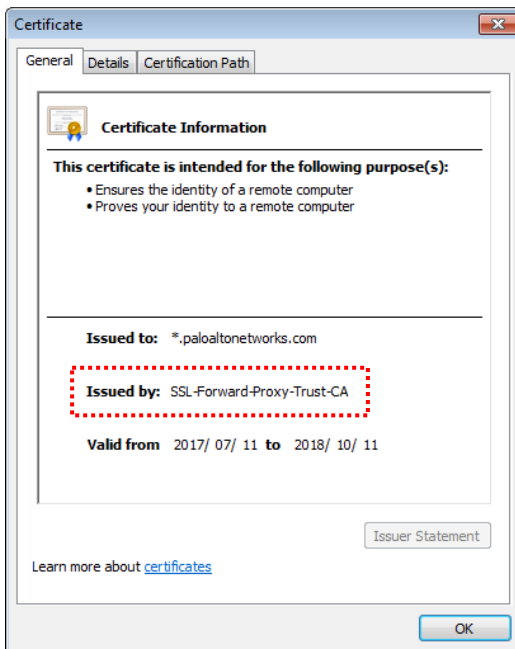


7.9.2.2. 金融系以外の Web サイトへアクセス

- (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。



- (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。



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。



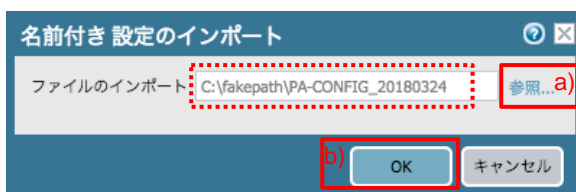
8.2.2. インポート

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。



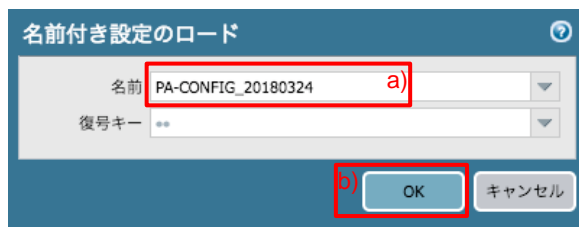
8.3. スナップショットのロード

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。

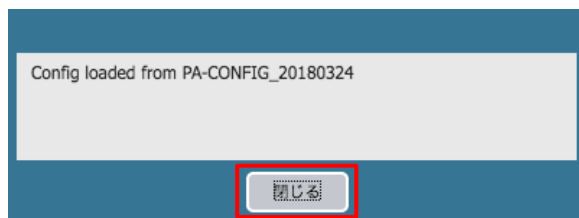
(1) 「名前付き 設定スナップショットのロード」をクリックします。



(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。



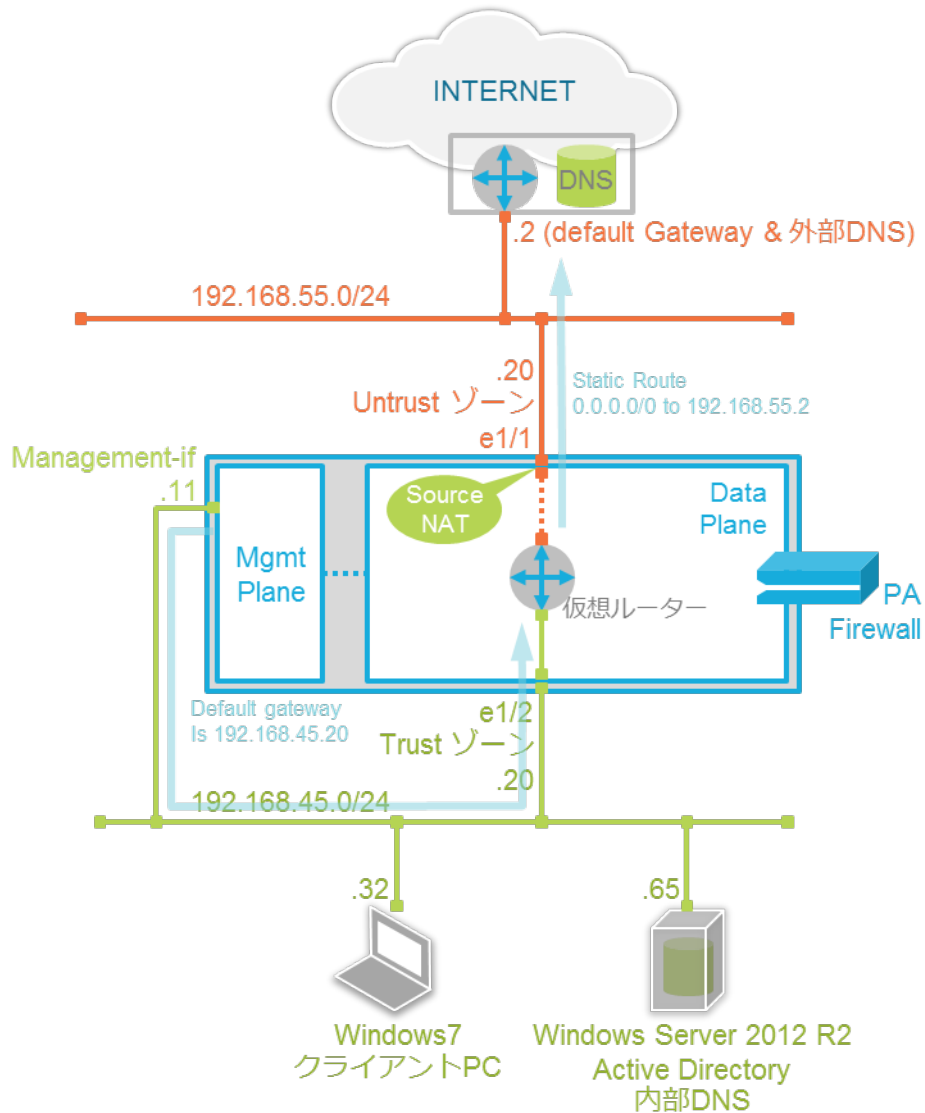
(3) 「閉じる」をクリックします。ロードが完了し、その時点までのコンフィグに戻っています。



9. ネットワーク構成の変更

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。

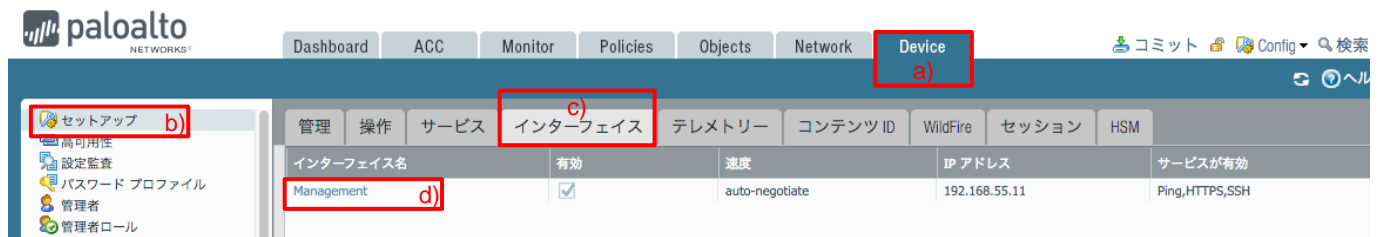
9.1. 変更後のネットワーク構成



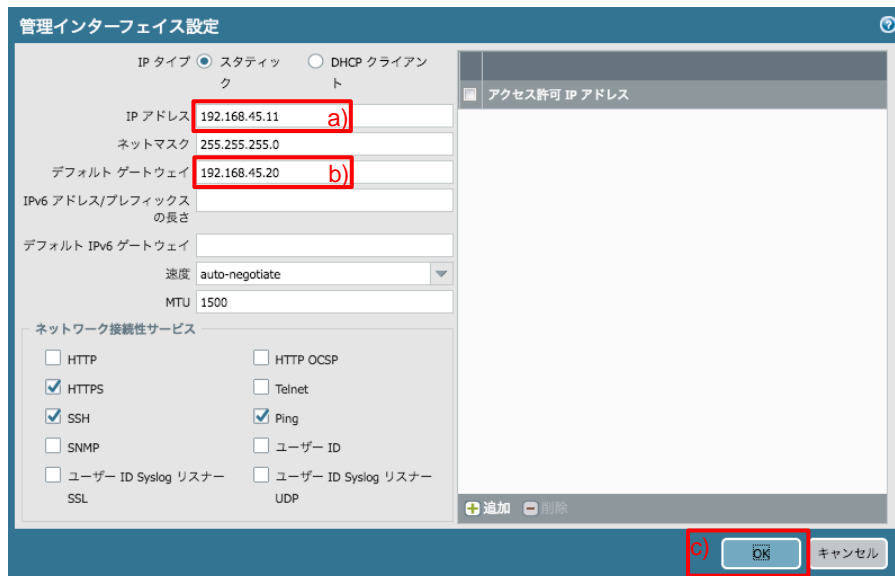
PA FirewallのマネージメントインターフェイスのIPアドレスを、192.168.45.11、デフォルトゲートウェイを192.168.45.20に変更し、Trustゾーン側のネットワークに接続し直します。

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」 → b)「セットアップ」 → 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。

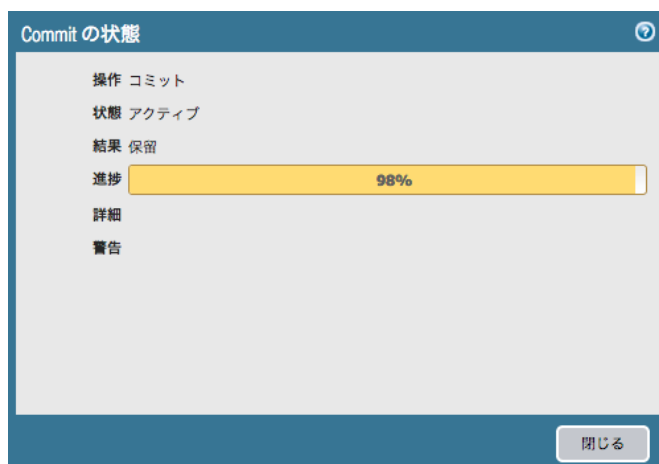


(2) ネットワーク構成に従って a)IP アドレスを「192.168.45.11」、b)デフォルトゲートウェイを「192.168.45.20」に変更します。c)「OK」をクリックします。



(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。



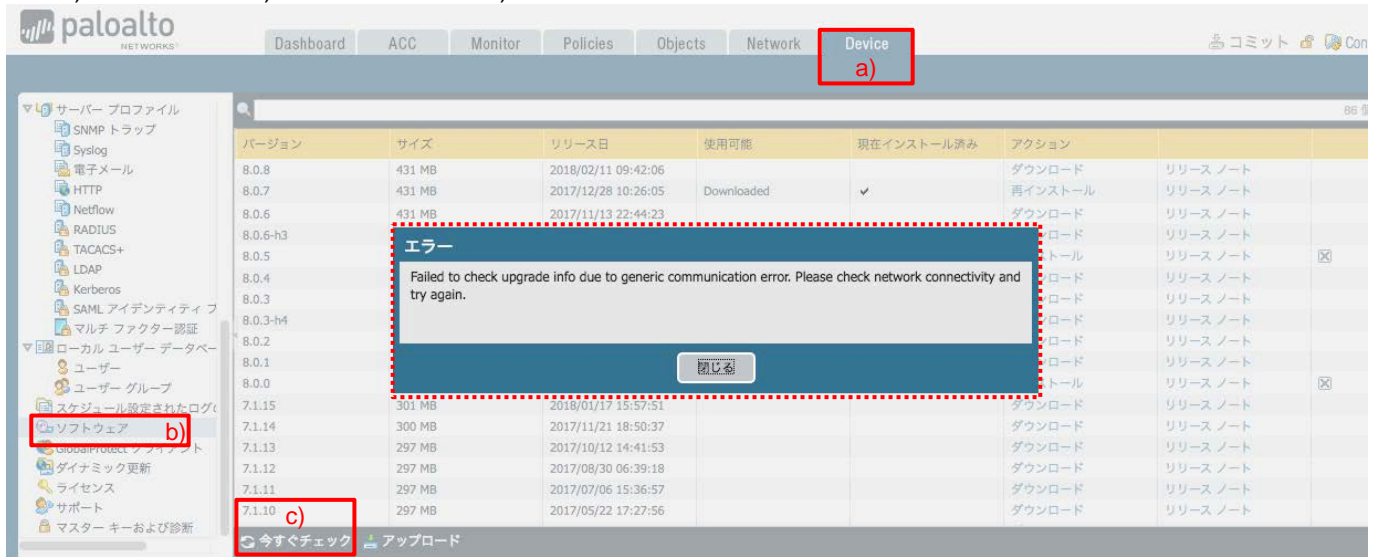
(5) マネージメントインターフェイスを Untrust ゾーンから物理的に切断し、Trust ゾーンへ接続します。

(6) Web ブラウザで、<https://192.168.45.11> へ接続し、WebUI が応答することを確認します。

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

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。

例: a)「Device」 → b)「ソフトウェア」 → 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 <https://updates.paloaltonetworks.com> へアクセスする際、「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。

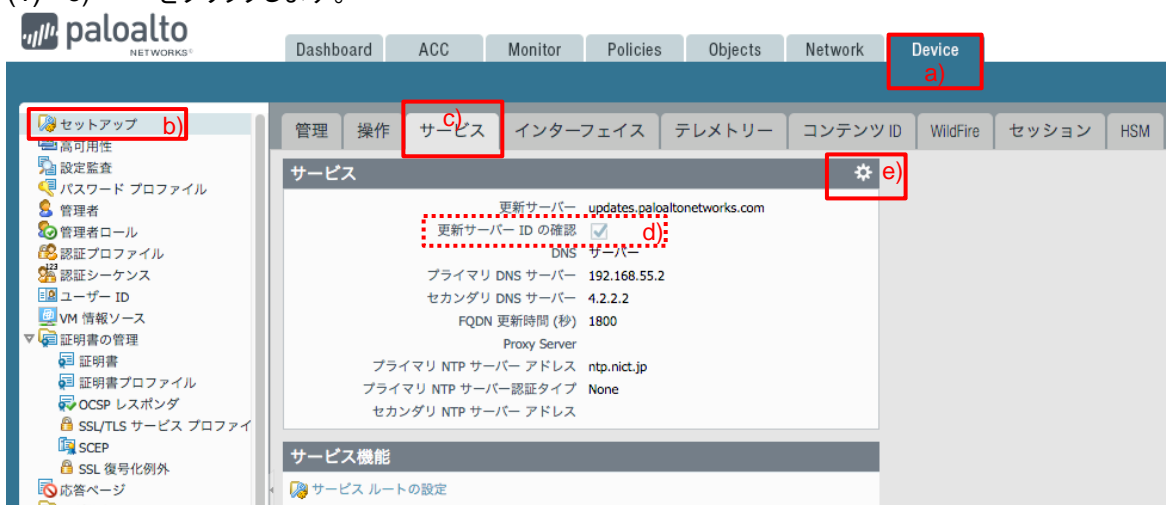
この状態を回避する策を 3 つ紹介します。

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

一つめの方法は、a)「Device」 → b)「セットアップ」 → 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。



(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」 → b)「ソフトウェア」 → 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ります。

結果、この方法を使うと、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。



(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」 → b)「ソフトウェア」 → 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。



- (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。



- (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」 → b)「ソフトウェア」 → 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、service-http 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なります。

(1) a)「Objects」 → b)「サービス」 → 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。

The screenshot shows the 'Service' configuration form. The 'Name' field is set to 'http' and is labeled 'a)'. The 'Protocol' field has 'TCP' selected, labeled 'b)'. The 'Destination Port' field is set to '80' and is labeled 'c)'. At the bottom right, the 'OK' button is highlighted with a red box and labeled 'd)'. The 'Cancel' button is also visible.

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。

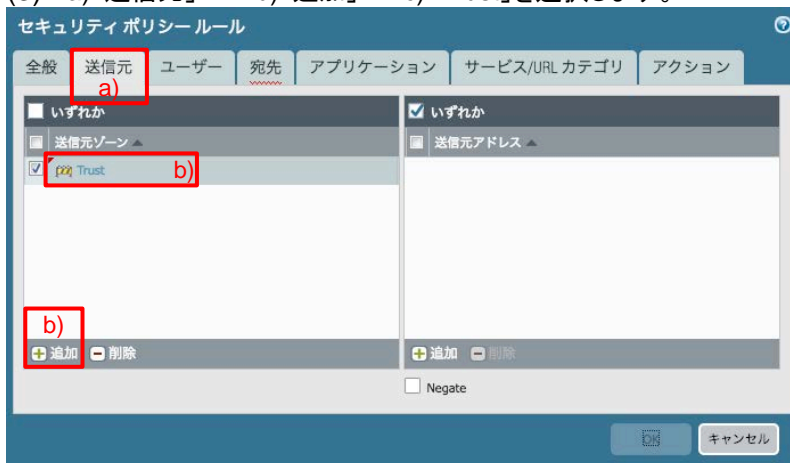
(1) a)「Policies」 → b)「セキュリティ」 → c)「追加」をクリックします。



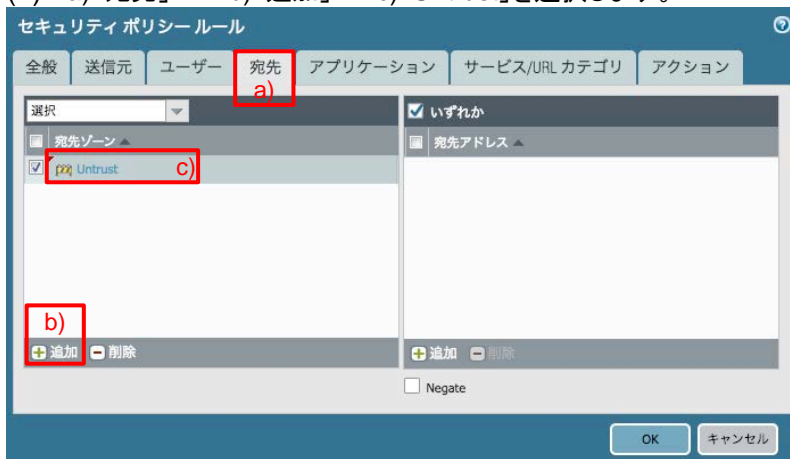
(2) a)「全般」 → b)名前に「allow outbound web (任意)」と入力します。



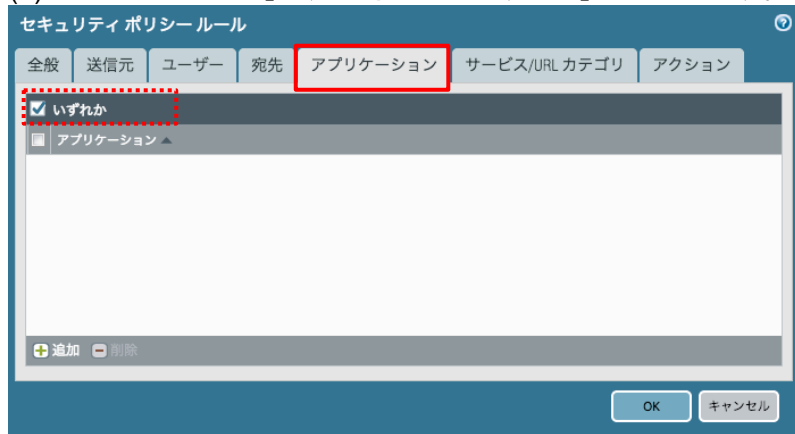
(3) a)「送信元」 → b)「追加」 → c)「Trust」を選択します。



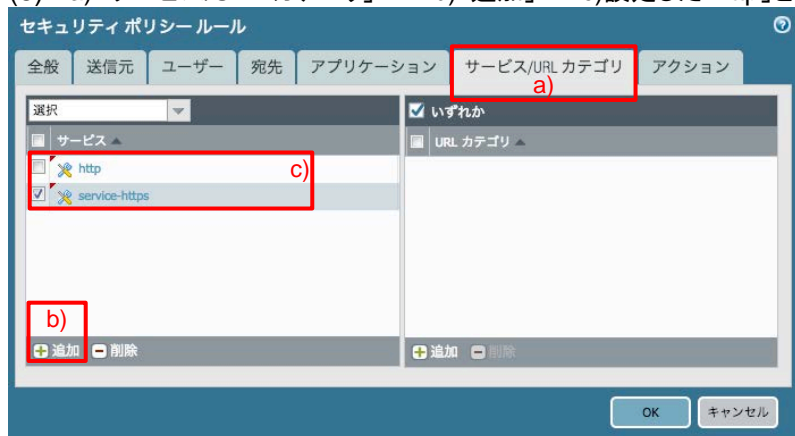
(4) a)「宛先」 → b)「追加」 → c)「Untrust」を選択します。



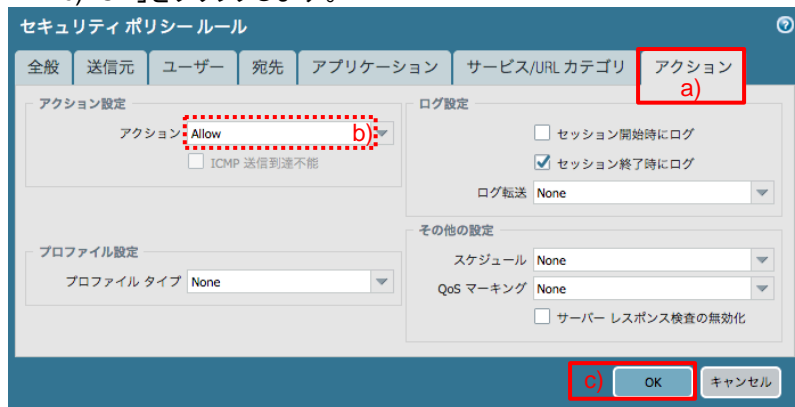
(5) 「アプリケーション」は、デフォルトの「いずれか」のままにします。



(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。



(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。



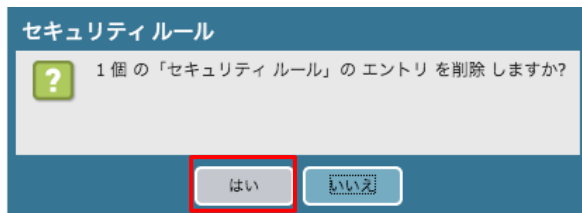
10.1.3. 全許可ポリシーの削除

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。



(2) 「はい」をクリックします。



(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。



10.2. Interzone-default の設定変更

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。

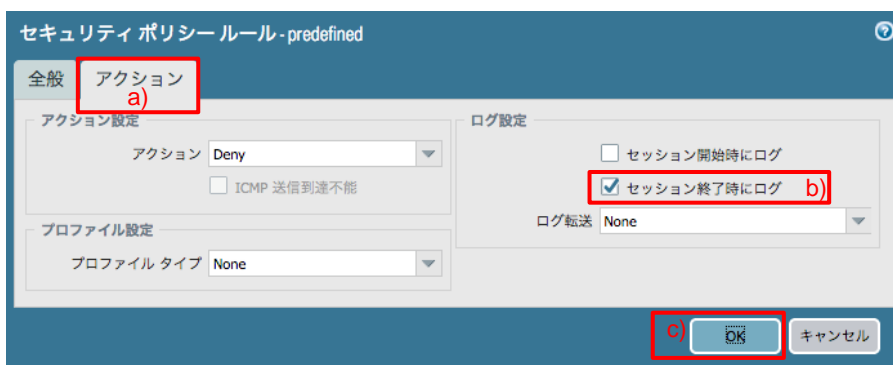
このポリシーは、ゾーン間通信を全て拒否するポリシーで、順番としては最後に評価されますが、ログ出力が無効になっています。

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な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。



(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。



(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なります。

[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。

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
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
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
02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:05	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:04	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:03	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:03	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:03	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:02	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:02	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
02/08 00:08:02	end	Trust	Untrust	192.168.45.65		192.168.55.2	53	dns	allow	allow outbound	aged-out
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なります。

11.1.1. 設定

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

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 web	none	universal	Trust	any	any	any	Untrust	any	any	http service-https	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	

(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

名前 **DNS**

ルールタイプ universal (default)

内容

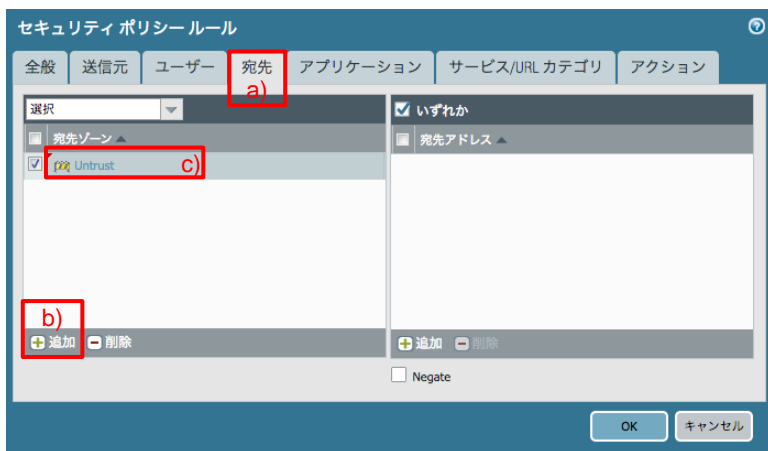
タグ

キャンセル

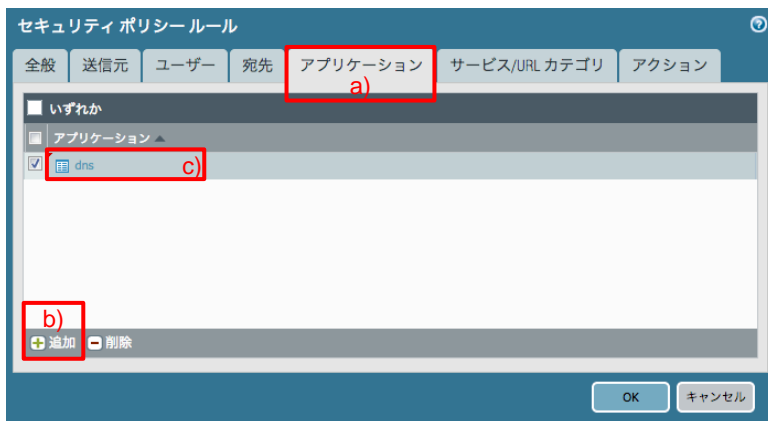
(3) a)「送信元」 → b)「追加」 → c)「Trust」を選択します。



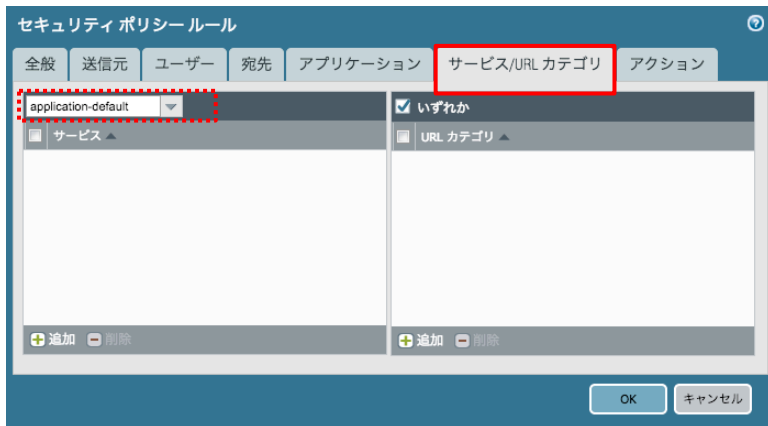
(4) a)「宛先」 → b)「追加」 → c)「Untrust」を選択します。



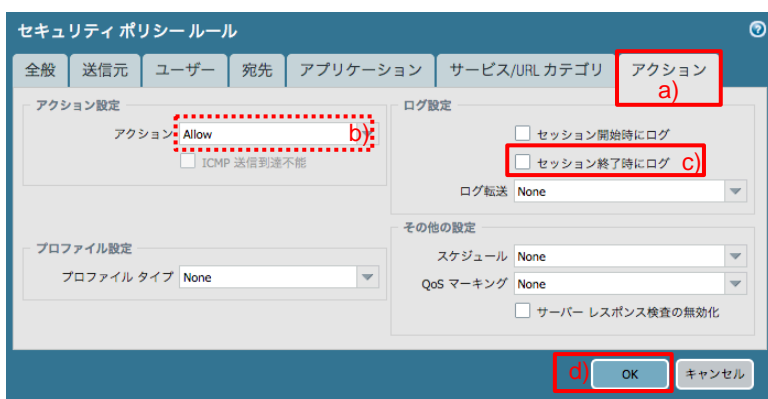
(5) a)「アプリケーション」 → b)「追加」で表示されたフォームに c)「dns」と入力して、「dns」を選択します。



(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。)



(7) a)「アクション」 → 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。



(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。



(9) 以下が DNS を上に移動した状態です。



(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)

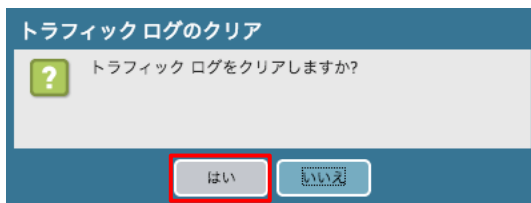
11.1.2. Traffic ログのクリア

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」 → 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。



- (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。



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。

The screenshot shows the Palo Alto Networks Objects management interface. The 'Objects' tab is selected. A search bar contains 'dns'. The left sidebar shows the 'Applications' category selected. The main area displays a table of search results for 'dns'.

名前	タグ付けされました	カテゴリ	サブカテゴリ	リスク	テクノロジー
<input type="checkbox"/> adnstream		media	photo-video	3	browser-based
<input checked="" type="checkbox"/> dns		networking	infrastructure	4	network-protocol
<input type="checkbox"/> dnscrypt		networking	infrastructure	1	client-server

- (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。

The screenshot shows the details page for the 'dns' application. The '標準ポート' (Standard Port) field is highlighted with a red dashed box, showing 'tcp/53, udp/53,5353'. Other fields include '名前: dns', '内容: The Domain Name System (DNS) stores and associates many types of information with domain names...', '追加情報: Wikipedia Google Yahoo!', '依存:', '特徴', '分類', and 'オプション'.

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。)



- (2) 「全般」の名前に「NTP(任意)」と入力します。



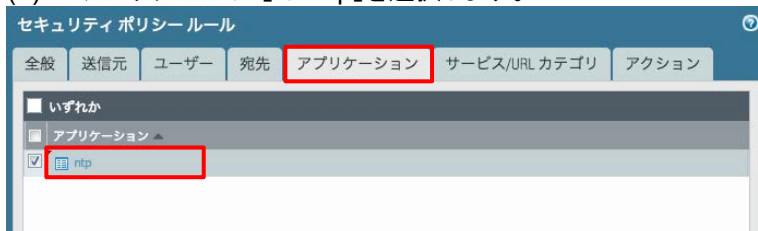
- (3) 「送信元」は「Trust」を選択します。



- (4) 「宛先」は「Untrust」を選択します。



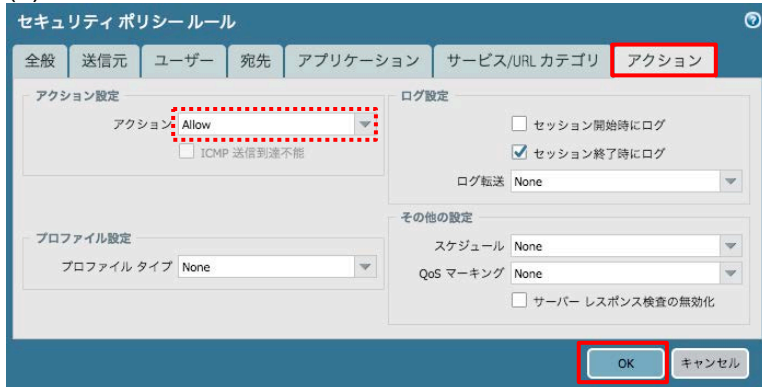
- (5) 「アプリケーション」は「ntp」を選択します。



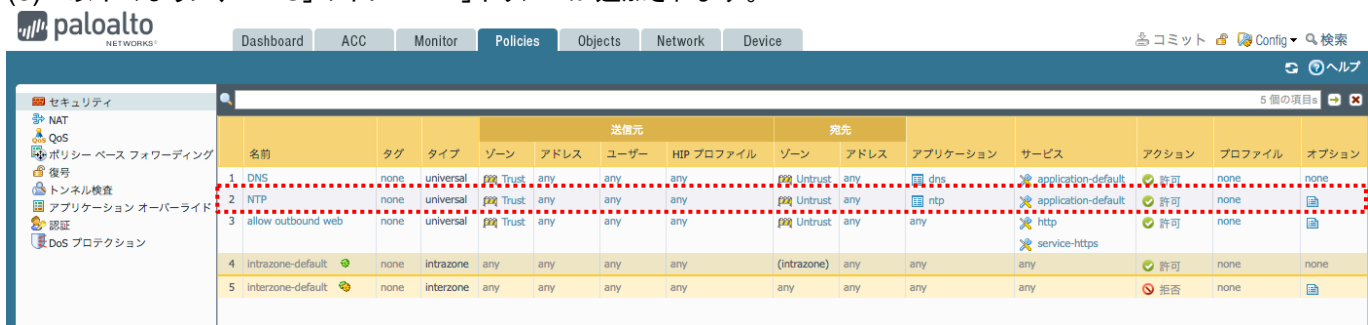
(6) 「サービス/URL カテゴリ」は「application-default」を選択します。



(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。



(8) 以下のように、「DNS」の下に「NTP」ポリシーが追加されます。



(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。
(c)のフォームに「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。)



(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りたいので、c)「NTP」を選択した状態で、d)「追加」をクリックします。



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



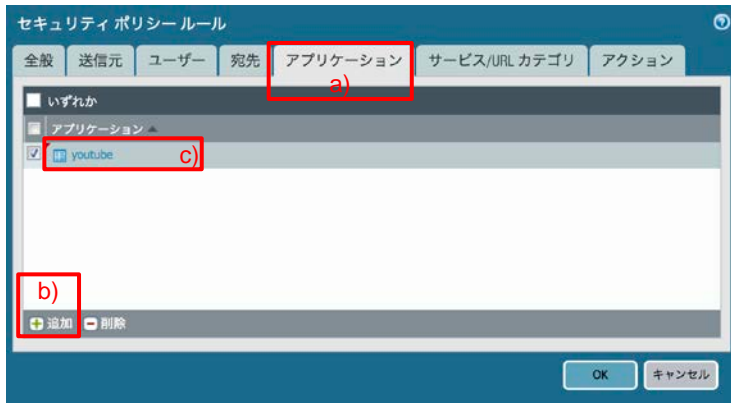
- (3) 「送信元」は「Trust」を選択します。



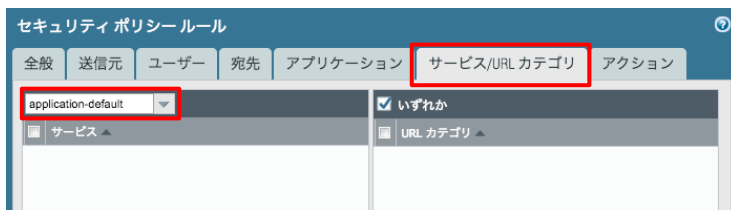
- (4) 「宛先」は「Untrust」を選択します。



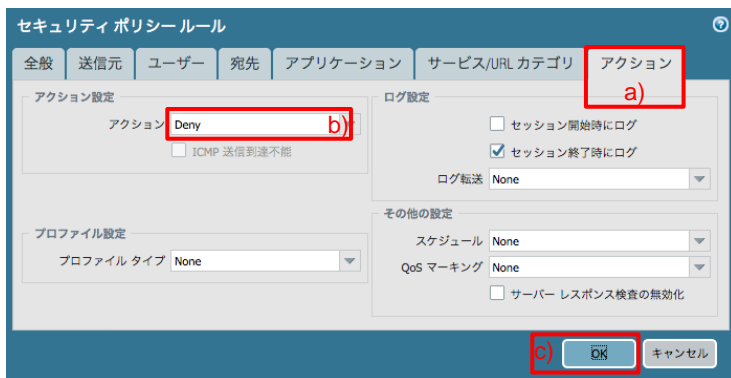
(5) a)「アプリケーション」 → b)「追加」で表示されたフォームに「youtube」と入力して、c)「youtube」を選択します。



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



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



(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。

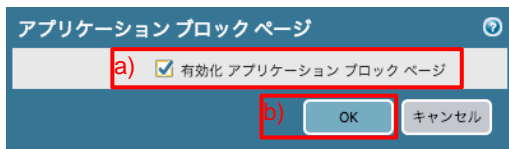
名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
1 DNS	none	universal	Trust	any	any	any	Untrust	any	dns	application-default	許可	none	none
2 NTP	none	universal	Trust	any	any	any	Untrust	any	ntp	application-default	許可	none	none
3 Youtube	none	universal	Trust	any	any	any	Untrust	any	youtube	application-default	拒否	none	none
4 allow outbound web	none	universal	Trust	any	any	any	Untrust	any	http	service-https	許可	none	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	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。



(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。

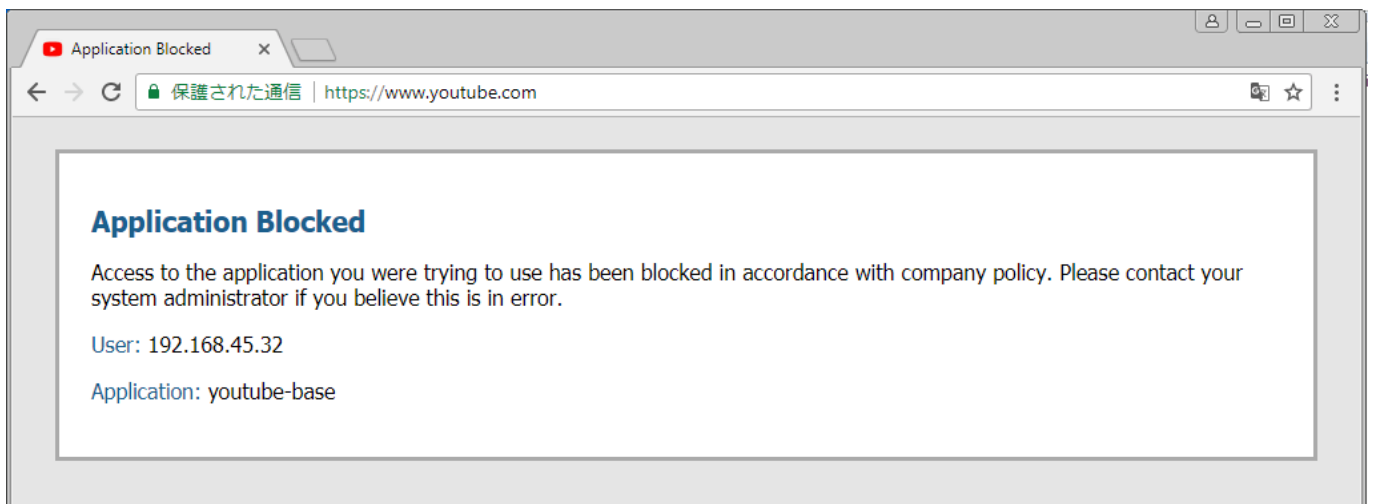


(11) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.4.2. 通信確認

(1) クライアント PC から、YouTube (www.youtube.com) へアクセスします。

(2) ブロックページが表示されます。



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」 → 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。



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



(3) 「送信元」は「Trust」を選択します。

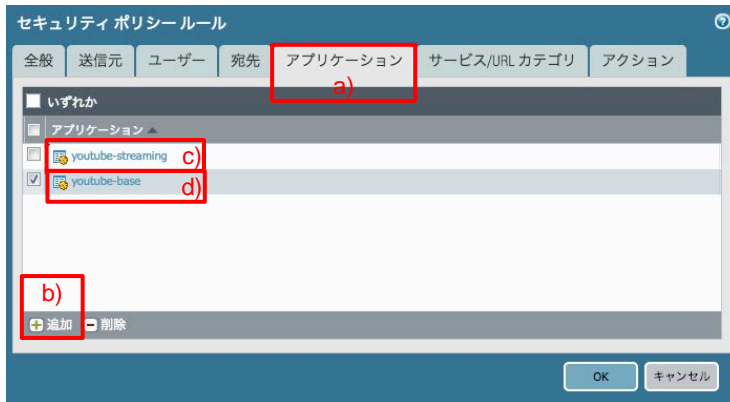


(4) 「宛先」は「Untrust」を選択します。

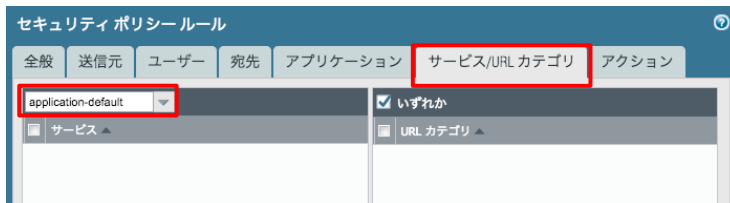


- (5) a)「アプリケーション」 → b)「追加」で表示されたフォームに「youtube-streaming」と入力して表示された、
c)「youtube-streaming」を選択します。
さらにもう一度、b)「追加」で表示されたフォームに「youtube-base」と入力して表示された、d)「youtube-base」を選択
します。

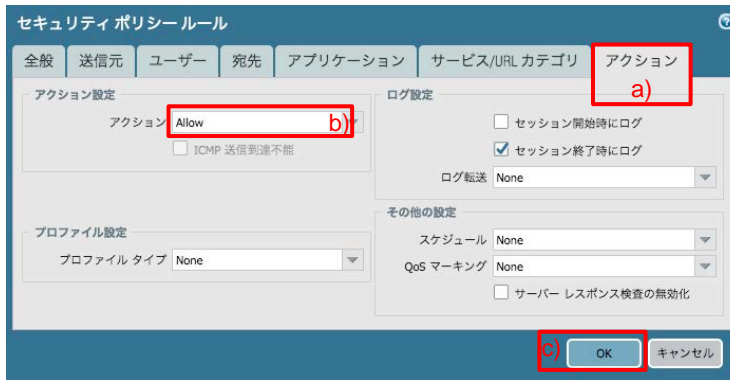
※ ここで2つのアプリケーションを選択した理由は、アプリケーションによっては「依存関係」が存在するためです。
アプリケーションの依存関係については後述します。



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



- (7) a)「アクション」 → 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。

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
2 NTP	none	universal	Trust	any	any	any	Untrust	any	ntp	application-default	許可	none	none
3 Youtube-streaming	none	universal	Trust	any	any	any	Untrust	any	youtube-base youtube-streaming	application-default	許可	none	none
4 Youtube	none	universal	Trust	any	any	any	Untrust	any	youtube	application-default	拒否	none	none
5 allow outbound web	none	universal	Trust	any	any	any	Untrust	any	any	http service-https	許可	none	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	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)

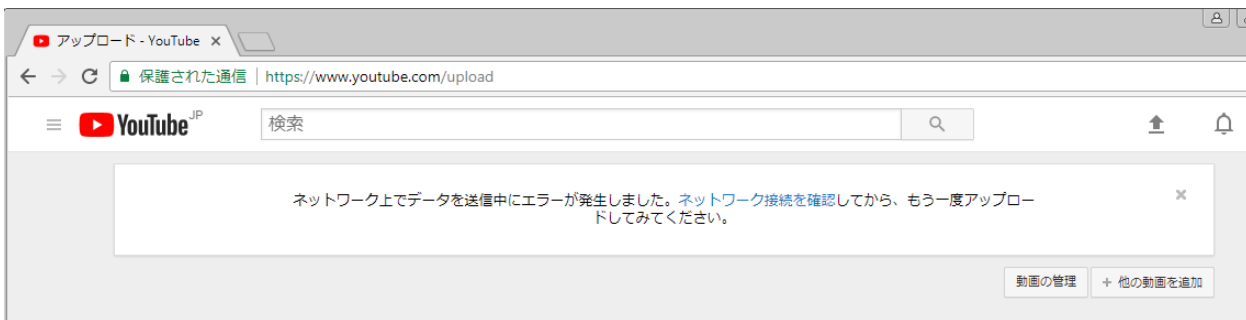
11.5.2. 通信確認

- (1) クライアント PC から YouTube (www.youtube.com) へアクセスし、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。



- (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

トラフィック ログ

	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
トラフィック	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
URL フィルタリング	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
WildFireへの送信	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
データ フィルタリング	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
HIP マッチ	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
ユーザー ID	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	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
設定	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
システム	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
アラーム	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	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
統合済み	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
パケット キャプチャ	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
アプリケーション スコープ	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	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	02/08 01:20:41	end	Trust	Untrust	192.168.45.32		172.217.31.131	443	tcp	google-base	allow	allow outbound web	tcp-fin
脅威モニター	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
脅威マップ	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
ネットワーク モニター	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
トラフィック マップ	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
セッション ブラウザ	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
ポットネット													
PDF レポート													
DNF サマリーの管理													

(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。



The screenshot shows the Palo Alto Networks firewall management interface. The 'Monitor' tab is active, displaying a log table for denied traffic. The table has columns for '受信日時' (Received Time), 'タイプ' (Type), '送信元ゾーン' (Source Zone), '宛先ゾーン' (Destination Zone), '送信元' (Source IP), '送信元ユーザー' (Source User), '宛先' (Destination IP), '宛先ポート' (Destination Port), 'IP プロトコル' (IP Protocol), 'アプリケーション' (Application), 'アクション' (Action), 'ルール' (Rule), 'セッション終了理由' (Session Termination Reason), and 'バイト' (Bytes). The logs show multiple entries for denied traffic with the application set to 'not-applicable' and the action set to 'deny'.

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	バイト
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
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
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
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
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
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。



- (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。



(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すが、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。

名前	タグ	タイプ	送信元				宛先		アプリケーション	サービス	アクション
			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			
1 DNS	none	universal	Trust	any	any	any	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 youtube-streaming	application-default	許可
4 Youtube	none	universal	Trust	any	any	any	Untrust	any	youtube	application-default	拒否
5 allow outbound web	none	universal	Trust	any	any	any	Untrust	any	any	http service-https	許可

「youtube」に、「youtube-base」アプリケーションが含まれている。

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

アプリケーション

名前: youtube-base

標準ポート: tcp/80,443

依存: google-base

暗黙的に使用:

追加情報: [Wikipedia](#) [Google](#) [Yahoo!](#)

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. Based on recent research we have noticed that for the photo-upload function to work properly on youtube, customers will 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。

名前	タグ	タイプ	送信元				宛先		アプリケーション	サービス	アクション
			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			
1 DNS	none	universal	Trust	any	any	any	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 youtube-streaming	application-default	許可
4 Youtube	none	universal	Trust	any	any	any	Untrust	any	youtube	application-default	拒否
5 allow outbound web	none	universal	Trust	any	any	any	Untrust	any	any	http service-https	許可

「any」に、「google-base」アプリケーションが含まれている。

11.7. リスク 5 の File Sharing をまとめて拒否する

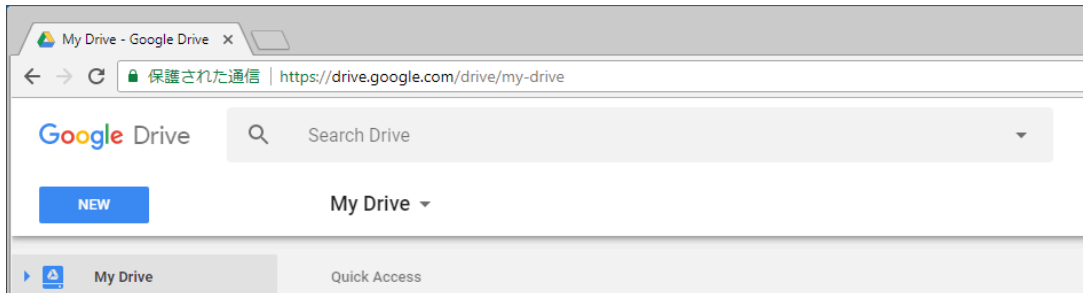
アプリケーションにはそれぞれパロアルトネットワークス社が定めた 5 段階のリスク値が設定されていて、5 がもっともリスクが高いアプリケーションである、という位置付けになっています。

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。

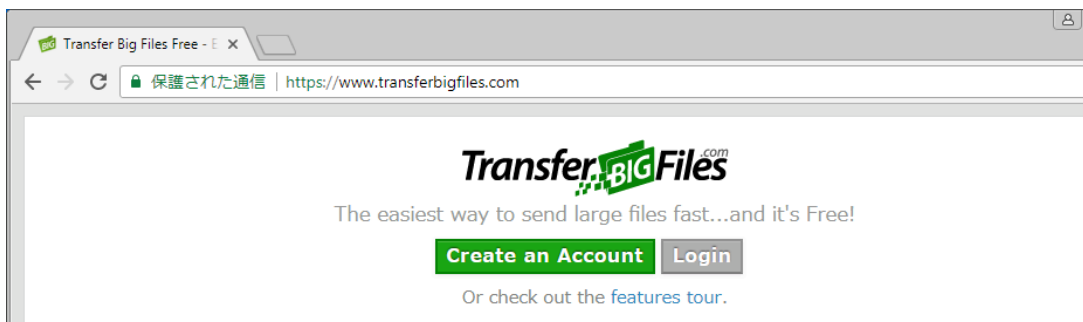
11.7.1. 設定前の通信確認

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>) へ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 (<https://www.transferbigfiles.com>) へアクセスできることを確認します。



11.7.2. 設定

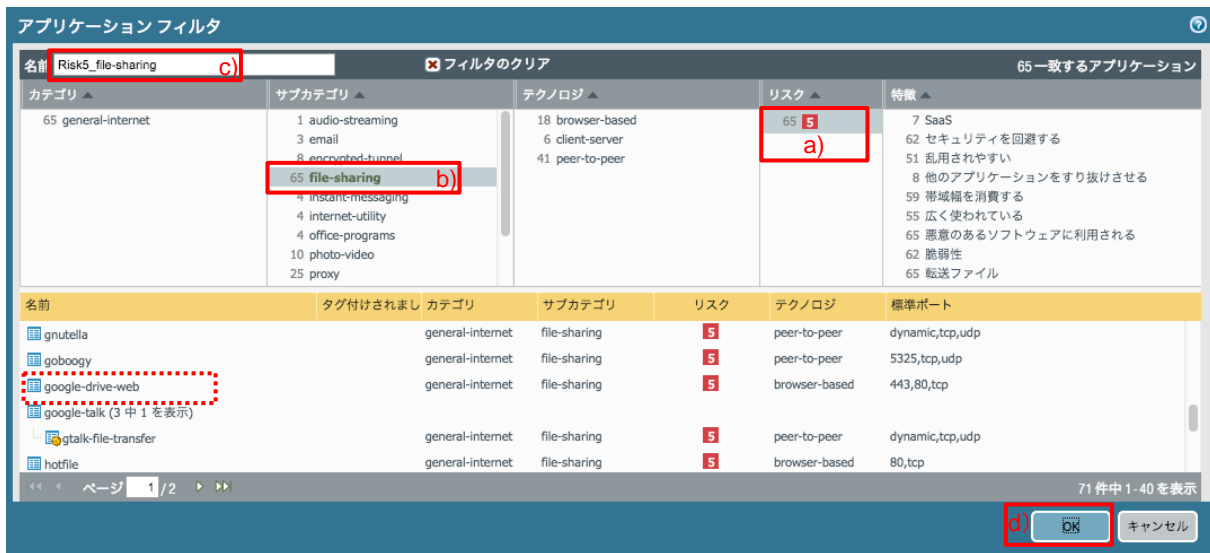
(1) a)「Objects」 → b)「アプリケーション フィルタ」 → c)「追加」 をクリックします。



(2) a)リスクの下に「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。)

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りたいので、c)「Youtube」を選択した状態で、d)「追加」をクリックします。



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



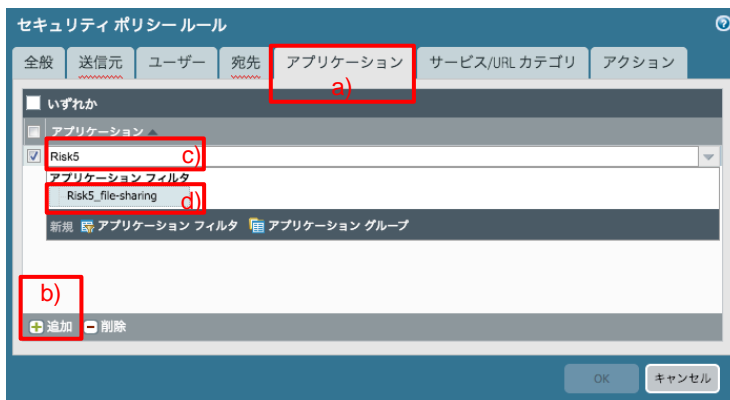
(5) 「送信元」は「Trust」を選択します。



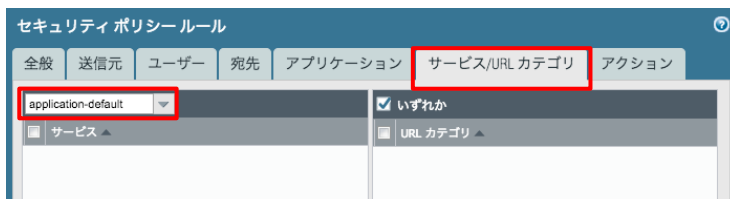
(6) 「宛先」は「Untrust」を選択します。



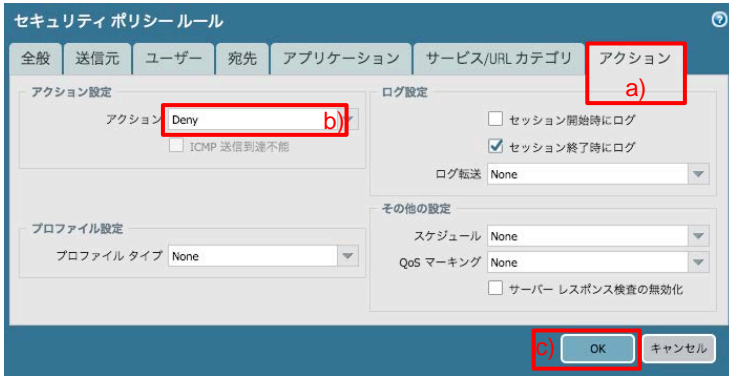
(7) a)「アプリケーション」 → b)「追加」で表示されたフォームに c)「Risk5」の文字列を入れて、作成したアプリケーションフィルタを検索します。表示された d)「Risk5_file-sharing」を選択します。



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



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



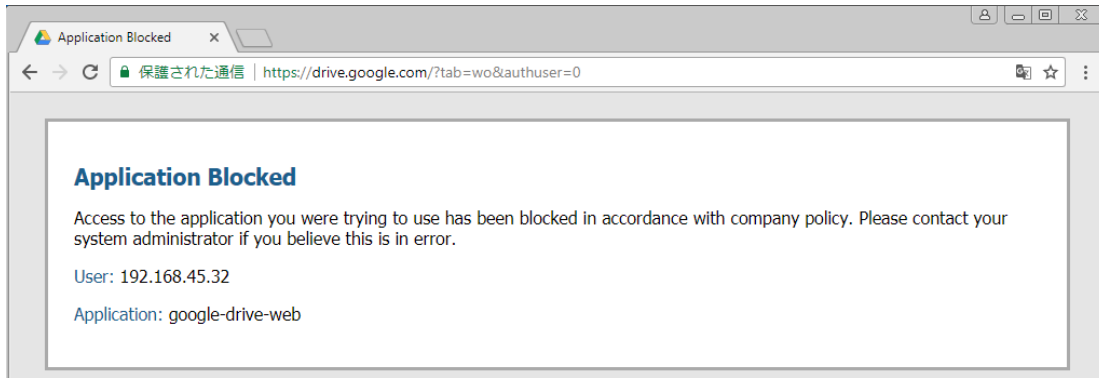
(10) 以下のように、「allow outbound web」ポリシーの上に「Risk5_file-sharing」を拒否するポリシーが追加されます。

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	any	Untrust	any	dns	application-default	許可	none	none
2 NTP	none	universal	Trust	any	any	any	any	Untrust	any	ntp	application-default	許可	none	none
3 Youtube-streaming	none	universal	Trust	any	any	any	any	Untrust	any	youtube-base	application-default	許可	none	none
4 Youtube	none	universal	Trust	any	any	any	any	Untrust	any	youtube	application-default	拒否	none	none
5 Risk5_file-sharing	none	universal	Trust	any	any	any	any	Untrust	any	Risk5_file-sharing	application-default	拒否	none	none
6 allow_outbound_web	none	universal	Trust	any	any	any	any	Untrust	any	any	http	許可	none	none
7 intrazone-default	none	intrazone	any	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	service-https	拒否	none	none

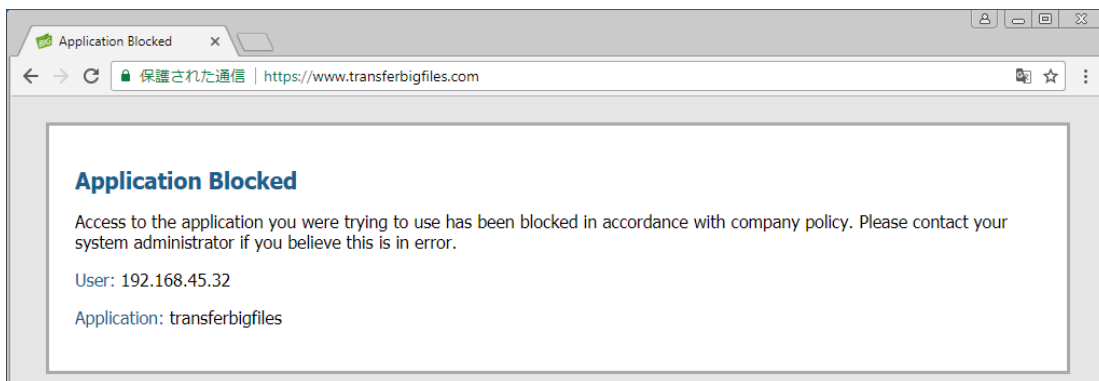
(11) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

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>) へアクセスすると、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>) へアクセスすると、拒否されることを確認します。



(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☑のフォームに c)「(rule eq Risk5_file-sharing)」の文字列が入ります。



11.8. リスク5 の File Sharing のうち、一つだけ許可する

「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りたいので、c)「Youtube」を選択した状態で、d)「追加」をクリックします。



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



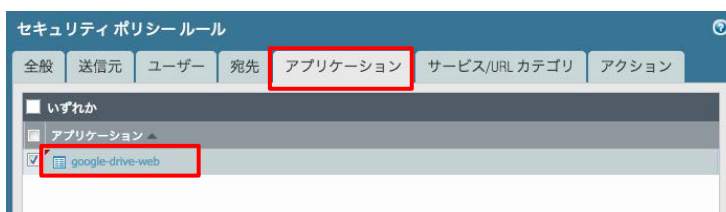
- (3) 「送信元」は「Trust」を選択します。



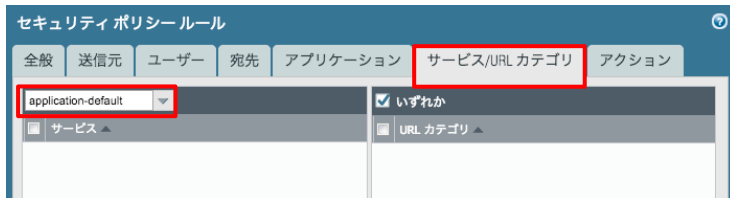
- (4) 「宛先」は「Untrust」を選択します。



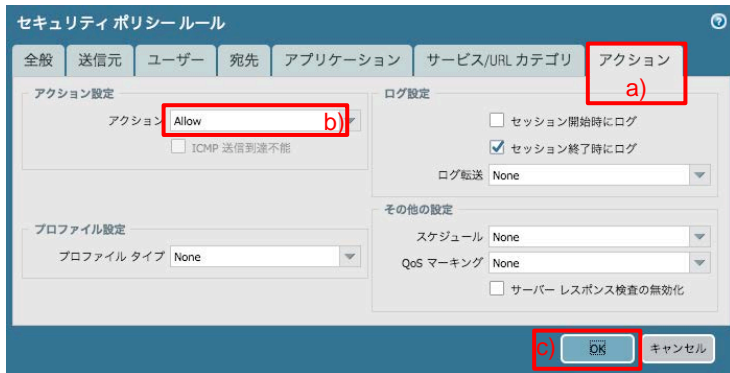
- (5) 「アプリケーション」は「google-drive-web」を選択します。



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



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



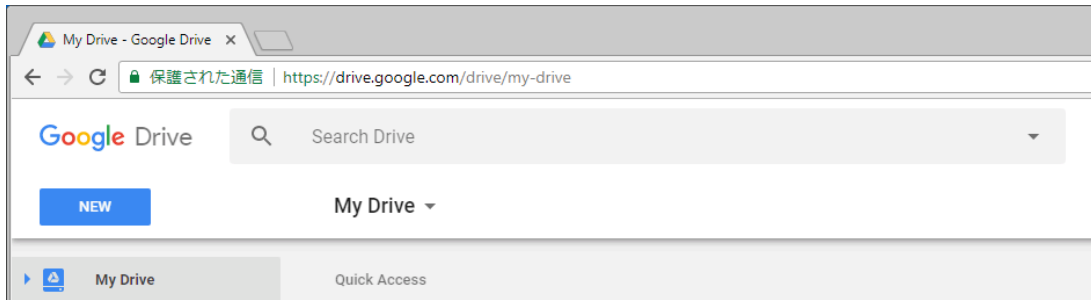
(8) 以下のように、「Risk5_file-sharing」ポリシーの上に「google-drive-web」を許可するポリシーが追加されます。

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
2 NTP	none	universal	Trust	any	any	any		Untrust	any	ntp	application-default	許可	none	none
3 Youtube-streaming	none	universal	Trust	any	any	any		Untrust	any	youtube-base	application-default	許可	none	none
4 Youtube	none	universal	Trust	any	any	any		Untrust	any	youtube	application-default	拒否	none	none
5 google-drive-web	none	universal	Trust	any	any	any		Untrust	any	google-drive-web	application-default	許可	none	none
6 Risk5_file-sharing	none	universal	Trust	any	any	any		Untrust	any	Risk5_file-sharing	application-default	拒否	none	none
7 allow outbound web	none	universal	Trust	any	any	any		Untrust	any	any	http	許可	none	none
8 intrazone-default	none	intrazone	any	any	any	any		(intrazone)	any	any	service-https	許可	none	none
9 interzone-default	none	interzone	any	any	any	any		any	any	any	拒否	none	none	

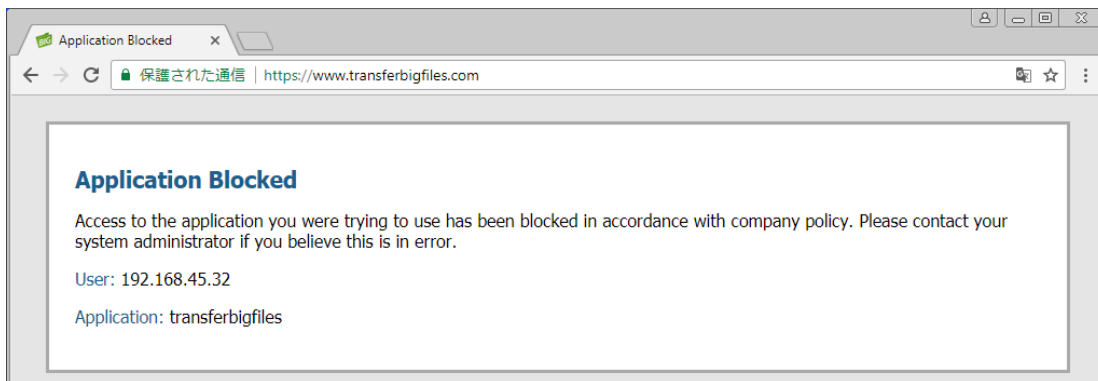
(9) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

11.8.2. 通信確認

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



(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、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。

A screenshot of the Palo Alto Networks Monitor page. The search bar contains the query "(rule eq google-drive-web) or (rule eq Risk5_file-sharing)". The table below shows traffic logs with columns for "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", and "バイト".

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	バイト
03/12 12:33:56	end	Trust	Untrust	192.168.45.32		kix05e01-in-f110.1e100.net	tcp	443	google-drive-web	allow	google-drive-web	tcp-fin	22.3k
03/12 12:33:54	end	Trust	Untrust	192.168.45.32		kix05e01-in-f110.1e100.net	tcp	443	google-drive-web	allow	google-drive-web	tcp-fin	135.3k
03/12 12:33:50	end	Trust	Untrust	192.168.45.32		kix05e07-in-f14.1e100.net	tcp	443	google-drive-web	allow	google-drive-web	tcp-fin	81.4k
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
03/12 12:33:27	deny	Trust	Untrust	192.168.45.32		tbfweb1.transferbigfiles.com	tcp	443	transferbigfiles	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 サイトへアクセスして、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 (<http://www.eicar.org/85-0-Download.html>) へアクセスします。
- (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。

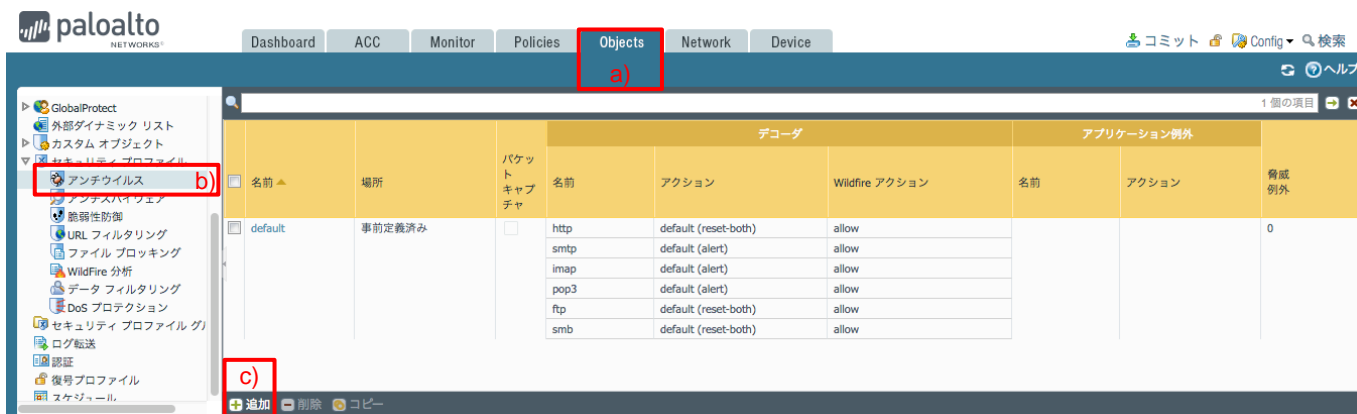
Download area using the standard protocol http			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
Download area using the secure, SSL enabled protocol https			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

※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。

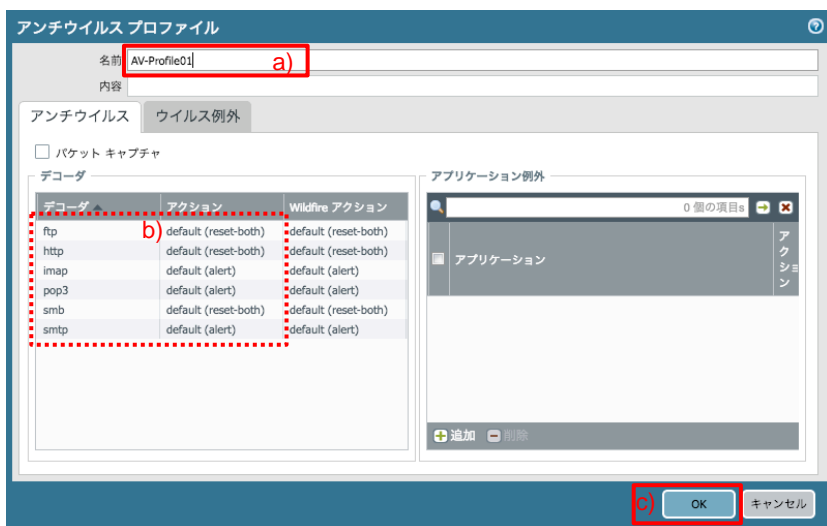
「クライアント PC で検知した」ということは「PA Firewall を通過してクライアント PC まで到達した」ということなので、PA Firewall のアンチウイルス設定前の動作確認としては、それで OK です。

12.1.2. 設定

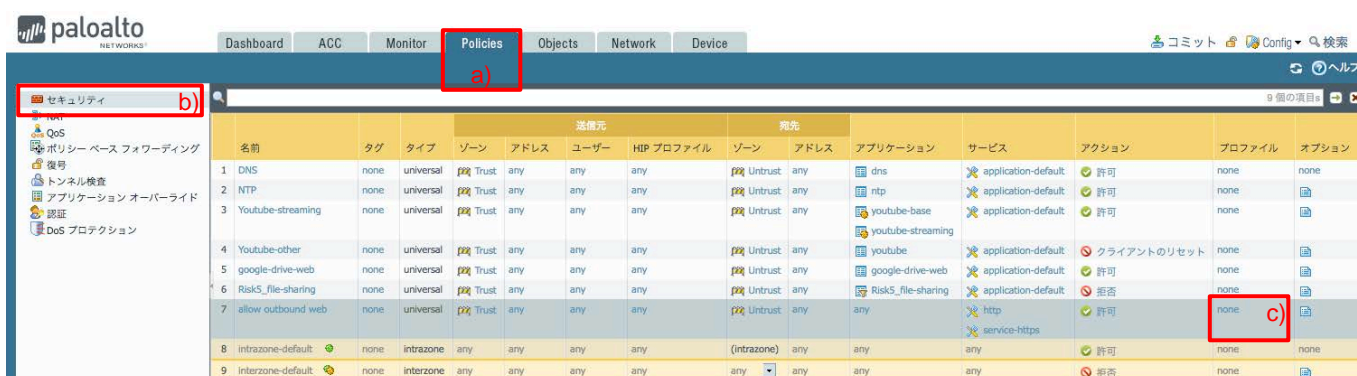
(1) a)「Objects」 → b)「アンチウイルス」 → c)「追加」をクリックします。



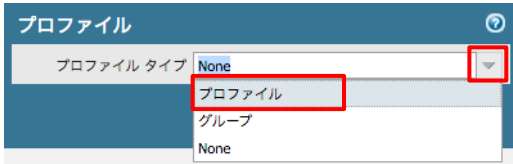
(2) a)名前に「AV-Profile01(任意)」と入力します。
デコーダに記載された http プロトコルのアクションが reset-both であることを確認し、c)「OK」をクリックします。
(その他のプロトコルのアクションもどのような設定になっているのか、確認しておいてください。)



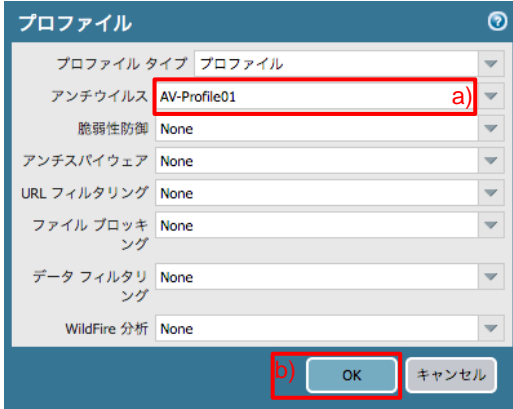
(3) a)「Policies」 → b)「セキュリティ」で表示された「allow outbound web」ポリシーの、プロファイル列 c)「none」をクリックします。



(4) プルダウンで、「プロファイル」を選択します。



(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。



(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。



(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)

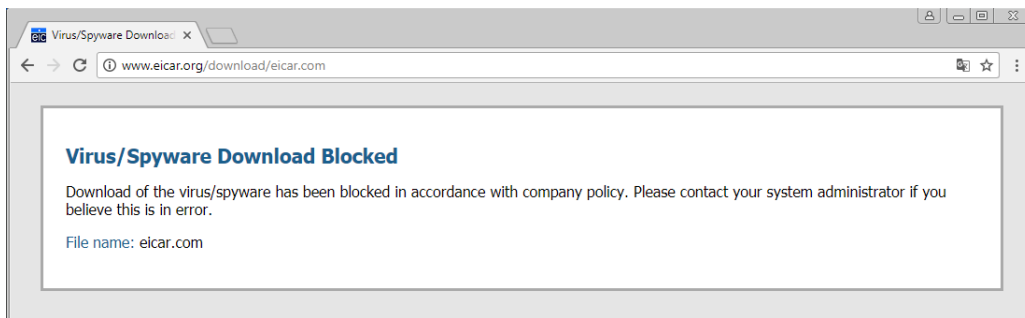
12.1.3. 動作確認

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

Download area using the standard protocol http			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Download area using the secure, SSL enabled 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)。



- (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。

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
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	
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	
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	
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。

全般	送信元	宛先
セッション ID 2122 アクション reset-both アプリケーション web-browsing ルール allow outbound web 仮想システム デバイスのシリアル番号 IP プロトコル tcp ログ アクション 生成日時 2018/03/12 17:11:29 受信日時 2018/03/12 17:11:29 トンネル タイプ N/A	攻撃者名 213.211.198.58 攻撃者 213.211.198.58 国 Germany ポート 443 ゾーン Untrust インターフェイス ethernet1/1 NAT IP 213.211.198.58 NAT ポート 443	被害者名 acme/user1 被害者 192.168.45.32 国 192.168.0.0-192.168.255.255 ポート 50032 ゾーン Trust インターフェイス ethernet1/2 NAT IP 192.168.55.20 NAT ポート 41828

詳細	
脅威タイプ	virus
脅威名	Eicar Test File
ID	90826973 (View in Threat Vault)
カテゴリ	js
コンテンツのパーソン	Antivirus-57611-61705
重大度	medium
繰り返し回数	1
ファイル名	eicar.com
URL	
PCAP ID	0
送信元 UUID	
宛先 UUID	

電子メール ヘッダ	
送信者のアドレス	
サブジェクト	

PCAP	受信日時 ▲	タイプ	アプリケーション	アクション	ルール	バイト	重大度	カテゴリ	判定	URL	ファイル名
	2018/03/12 17:11:37	end	web-browsing	allow	allow outbound web	5587		computer-and-internet-info			
	2018/03/12 17:11:29	virus	web-browsing	reset-both	allow outbound web		medium	computer-and-internet-info			eicar.com

※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」 → b)「脆弱性防御」 → c)「追加」をクリックします。

The screenshot shows the Palo Alto Networks configuration interface. The 'Objects' tab is selected and highlighted with a red box labeled 'a)'. In the left-hand navigation pane, '脆弱性防御' (Vulnerability Protection) is highlighted with a red box labeled 'b)'. At the bottom of the interface, the '+ 追加' (Add) button is highlighted with a red box labeled 'c)'. The main content area displays a table of vulnerability protection rules.

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			
strict	事前定義済み	ルール: 10	simple-client-critical	any	client	critical	reset-both	disable			
			simple-client-high	any	client	high	reset-both	disable			
			simple-client-medium	any	client	medium	reset-both	disable			
			simple-client-informational	any	client	informational	default	disable			
			simple-client-low	any	client	low	default	disable			
			simple-server-critical	any	server	critical	reset-both	disable			
			simple-server-high	any	server	high	reset-both	disable			
						詳細...					
			default	事前定義済み	ルール: 6	simple-client-critical	any	client	critical	default	disable
						simple-client-high	any	client	high	default	disable
simple-client-medium	any	client				medium	default	disable			
simple-server-critical	any	server				critical	default	disable			
simple-server-high	any	server				high	default	disable			
simple-server-medium	any	server				medium	default	disable			

(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。

The screenshot shows the '脆弱性防御プロファイル' (Vulnerability Protection Profile) configuration window. The '名前' (Name) field is set to 'VP-Profile01' and is highlighted with a red box labeled 'a)'. At the bottom left, the '+ 追加' (Add) button is highlighted with a red box labeled 'b)'. The window also shows a table for rules and an '例外' (Exceptions) tab.

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
------	-----	-----	---------	-----	-------	------------

- (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。

脆弱性防御ルール

ルール名 a)

脅威名 any

アクション デフォルト

パケット キャプチャ extended-capture b)

ホスト タイプ any

カテゴリ any

重大度

- any (All severities)
- critical c)
- high
- medium
- low
- informational

追加 削除

OK キャンセル

- (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。

脆弱性防御ルール

ルール名 a)

脅威名 any

アクション デフォルト

パケット キャプチャ disable b)

ホスト タイプ any

カテゴリ any

重大度

- any (All severities)
- critical
- high
- medium c)
- low
- informational

追加 削除

OK キャンセル

- (5) 「OK」をクリックします。

脆弱性防御プロファイル

名前

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	default	extended-capture
VP-Rule02	any	any	any	high	default	disable
				medium		
				low		
				informational		

追加 削除 上へ 下へ コピー 一致するシグネチャを検出

OK 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。



(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。



(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。



(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)

12.2.2. 動作確認

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: <https://www.google.co.jp>) で、以下の文字列を入力し、送信します。

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



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

Google 検索 I'm Feeling Lucky

Google が提供: English

(2) a)「Monitor」 → b)「脅威」でログを確認します。

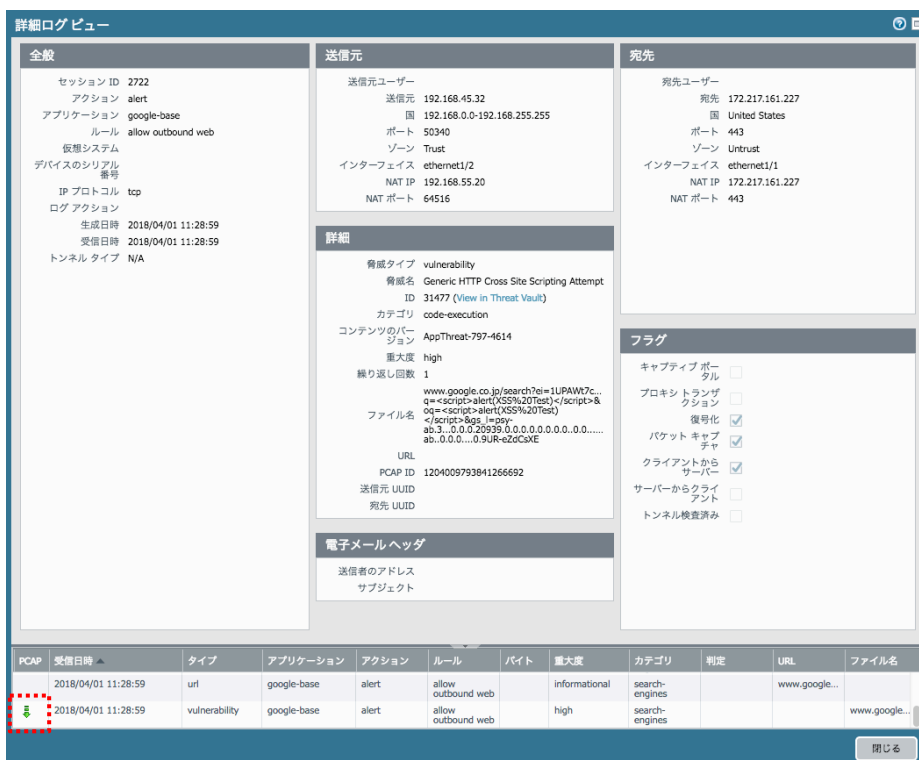
以下のように、タイプが「Vulnerability (脆弱性)」として検知した脅威ログが出力されます。



(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。



※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。

12.3. Wildfire

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。



(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。



(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) アイコンをクリックします。



12.3.2. 動作確認

(1) クライアントから、以下 Link へアクセスして、テスト用の未知マルウェ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。

The screenshot shows the Palo Alto Networks Monitor interface. The 'Monitor' tab is selected. A log entry is visible in the table below, with a red box highlighting the 'WildFireへの送信' (Send to WildFire) link in the left sidebar and another red box highlighting the 'malicious' verdict in the '判定' (Verdict) column of the log entry.

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
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

(5) 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。

(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。

※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。

12.4. ファイルブロッキング

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、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。

The screenshot shows the Palo Alto Networks management console. The 'Objects' tab is selected. In the left sidebar, 'ファイル ブロッキング' (File Blocking) is highlighted with a red box labeled 'b)'. The main table lists several rules. The rule 'basic file blocking' is selected with a checkmark and highlighted with a red box labeled 'c)'. At the bottom of the table, the 'コピー' (Copy) button is highlighted with a red box labeled 'd)'. The table data is as follows:

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		
<input checked="" type="checkbox"/>		basic file blocking	事前定義済み	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, oox, PE, pif, rar, scr, torrent, vbe, wsf	both	block
<input type="checkbox"/>				Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
<input type="checkbox"/>				Log all other file types	any	any	both	alert
<input type="checkbox"/>		strict file blocking	事前定義済み	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, Multi-Level-Encoding, oox, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
<input type="checkbox"/>				Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	block
<input type="checkbox"/>				Log all other file types	any	any	both	alert

- (2) 「OK」をクリックします。

The screenshot shows a 'コピー' (Copy) dialog box. It contains a list of selected objects with 'basic file blocking' listed. At the bottom, the 'OK' button is highlighted with a red box.

- (3) コピーされた「basic file blocking-1」をクリックします。

The screenshot shows the Palo Alto Networks management console after copying the rule. The 'basic file blocking-1' rule is now visible in the table and highlighted with a red box. The table data is as follows:

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		
<input type="checkbox"/>		basic file blocking-1		Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, oox, PE, pif, rar, scr, torrent, vbe, wsf	both	block
<input type="checkbox"/>				Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
<input type="checkbox"/>				Log all other file types	any	any	both	alert
<input type="checkbox"/>		basic file blocking	事前定義済み	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, oox, PE, pif, rar, scr, torrent, vbe, wsf	both	block
<input type="checkbox"/>				Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
<input type="checkbox"/>				Log all other file types	any	any	both	alert
<input type="checkbox"/>		strict file blocking	事前定義済み	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, Multi-Level-Encoding, oox, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
<input type="checkbox"/>				Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	block
<input type="checkbox"/>				Log all other file types	any	any	both	alert

(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。



(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。



(6) FB-Profile01 のファイルタイプは、以下の状態になります。

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
FB-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)プロフィール列にあるアイコンをクリックします。

名前	タグ	タイプ	送信元			宛先			アプリケーション	サービス	アクション	プロフィール	オプション
			ゾーン	アドレス	ユーザー	ゾーン	アドレス						
1 DNS	none	universal	Trust	any	any	Untrust	any	dns	application-default	許可	[Icons]	none	
2 NTP	none	universal	Trust	any	any	Untrust	any	ntp	application-default	許可	[Icons]	[Icon]	
3 Youtube-streaming	none	universal	Trust	any	any	Untrust	any	youtube-base	application-default	許可	[Icons]	[Icon]	
4 Youtube	none	universal	Trust	any	any	Untrust	any	youtube	application-default	拒否	none	[Icon]	
5 google-drive-web	none	universal	Trust	any	any	Untrust	any	google-drive-web	application-default	許可	[Icons]	[Icon]	
6 Risk5_file-sharing	none	universal	Trust	any	any	Untrust	any	Risk5_file-sharing	application-default	拒否	none	[Icon]	
7 allow outbound web	none	universal	Trust	any	any	Untrust	any	any	http	許可	[Icons]	[Icon]	
8 intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	許可	none	none	
9 interzone-default	none	interzone	any	any	any	any	any	any	any	拒否	none	[Icon]	

(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。

プロフィール

プロフィール 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 ブロッキング: **FB-Profile01** (a)

データ フィルタリング: None

WildFire 分析: WF-Profile01

OK (b) キャンセル

(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ィールを割り当てます。

名前	タグ	タイプ	送信元			宛先			アプリケーション	サービス	アクション	プロフィール	オプション
			ゾーン	アドレス	ユーザー	ゾーン	アドレス						
1 DNS	none	universal	Trust	any	any	Untrust	any	dns	application-default	許可	[Icons]	none	
2 NTP	none	universal	Trust	any	any	Untrust	any	ntp	application-default	許可	[Icons]	[Icon]	
3 Youtube-streaming	none	universal	Trust	any	any	Untrust	any	youtube-base	application-default	許可	[Icons]	[Icon]	
4 Youtube	none	universal	Trust	any	any	Untrust	any	youtube	application-default	拒否	none	[Icon]	
5 google-drive-web	none	universal	Trust	any	any	Untrust	any	google-drive-web	application-default	許可	[Icons]	[Icon]	
6 Risk5_file-sharing	none	universal	Trust	any	any	Untrust	any	Risk5_file-sharing	application-default	拒否	none	[Icon]	
7 allow outbound web	none	universal	Trust	any	any	Untrust	any	any	http	許可	[Icons]	[Icon]	
8 intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	許可	none	none	
9 interzone-default	none	interzone	any	any	any	any	any	any	any	拒否	none	[Icon]	

(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)

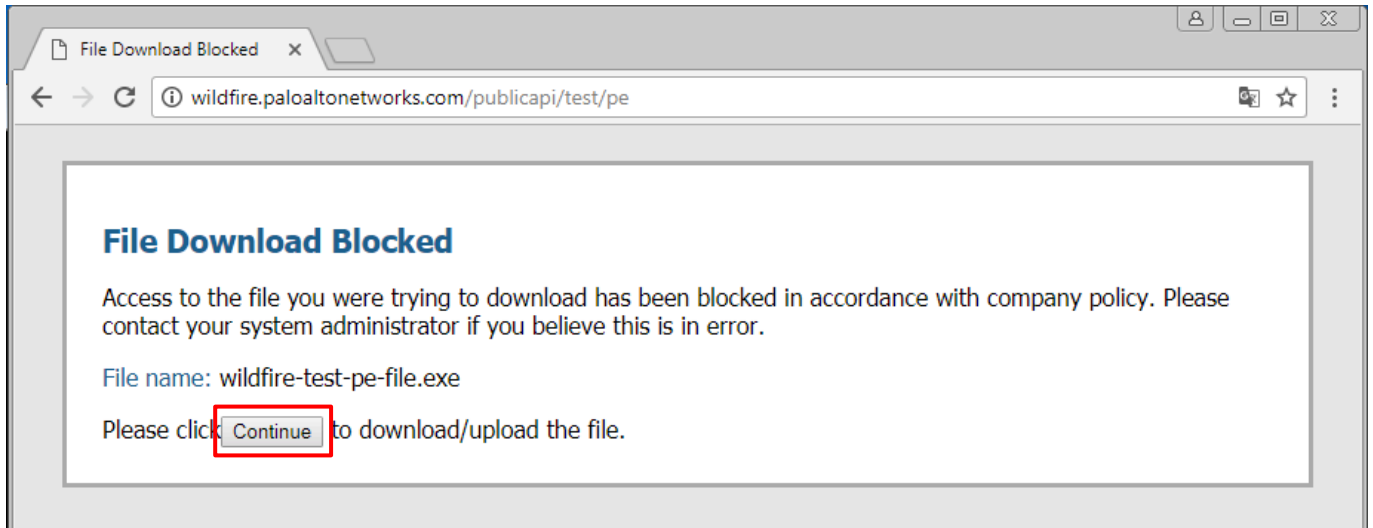
12.4.2. 動作確認

(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。



(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。



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。

一つ目は、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。

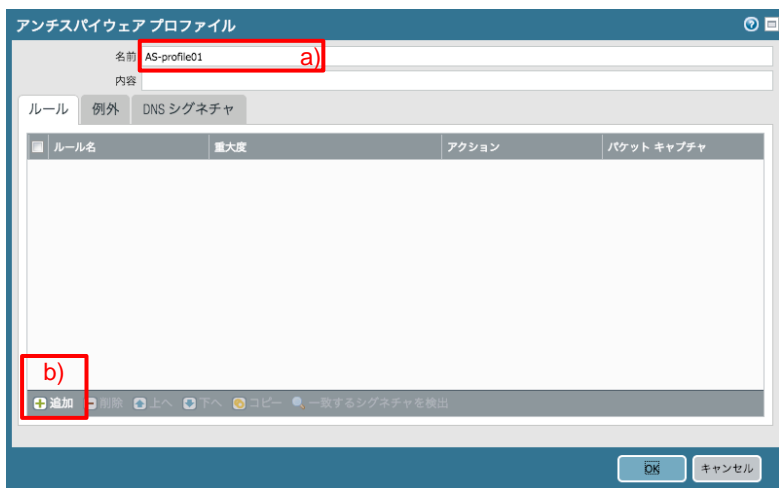
[DNSシンクホール]: クライアントからマルウェアサイトへのDNSリクエストが発せられた場合に、PA Firewallは、あらかじめ設定された偽りのIPアドレスをDNSレスポンスに入れて返答する機能のことです。

12.5.1. 設定

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



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



- (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なります。
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

ルール名 AS-Rule01 a)

脅威名 any
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照合に使用

カテゴリ any

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 severities)

critical c)

high

medium

low

informational

d) OK キャンセル

- (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。

アンチスパイウェアルール

ルール名 AS-Rule02 a)

脅威名 any
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照合に使用

カテゴリ any

アクション デフォルト

パケット キャプチャ disable b)

重大度

any (All severities)

critical

high

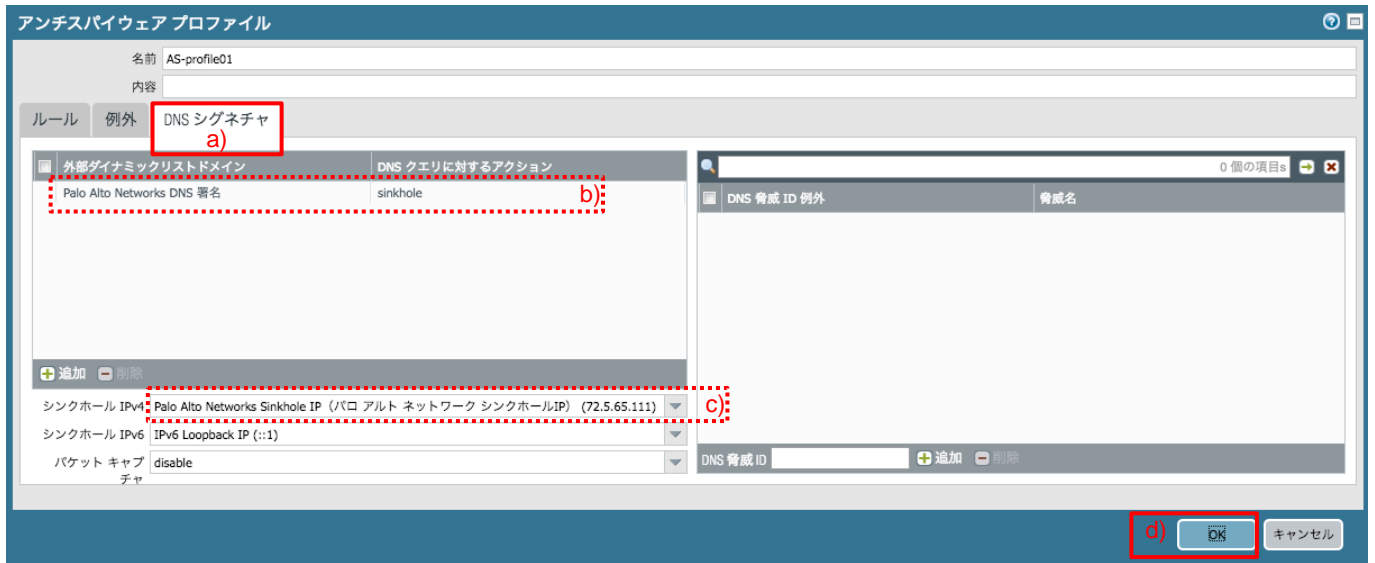
medium c)

low

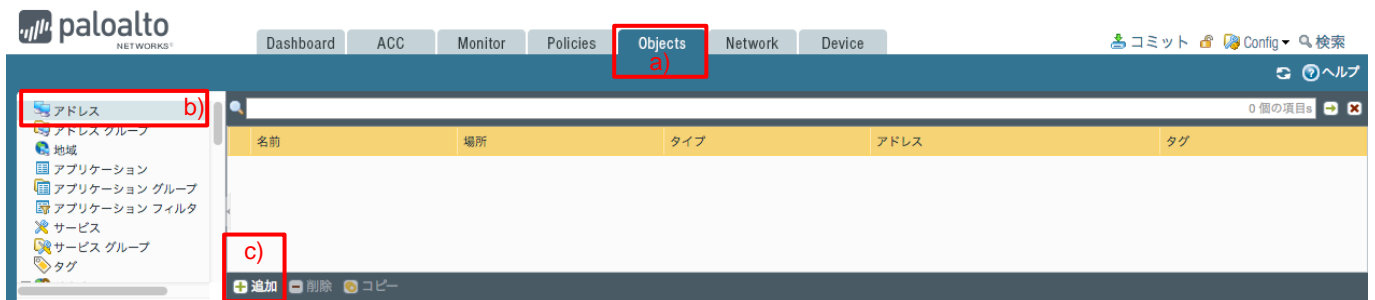
informational

d) OK キャンセル

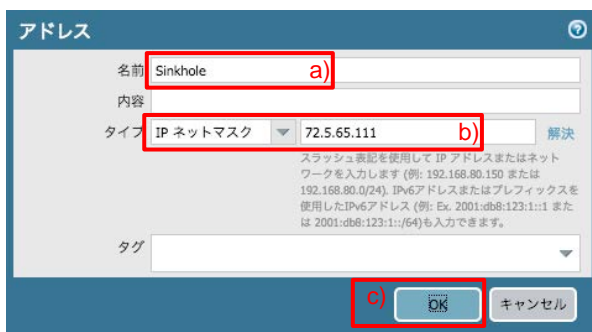
- (5) a)「DNS シグネチャ」タブをクリックします。
 b)が「sinkhole」となっていること及びシンクホール IPv4 が「72.5.65.111」に設定されていることを確認します。
 (IP アドレスは変更可能です。違うアドレスに変更したいときは、c)をクリックして上書きしてください。)
 d)「OK」をクリックします。



- (6) アドレスオブジェクトを登録しておく、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」 → b)「アドレス」 → c)「追加」をクリックします。



- (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。



(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。



(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。



(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。



(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。



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
▼ アンチウイルス 最終チェック: 2018/02/07 23:01:00 JST スケジュール: Every hour (Download and Install)									
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
2513-3009	panup-all-antivirus-2513-3009		Full	84 MB	2018/02/06 21:01:42 JST	▼	▼	ダウンロード	リリースノート
2511-3005	panup-all-antivirus-2511-3005		Full	85 MB	2018/02/03 21:04:44 JST			ダウンロード	リリースノート
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
▼ アプリケーションおよび脅威 最終チェック: 2018/02/08 00:48:47 JST スケジュール: Every hour at 0 minutes past the hour (Download and Install)									
777-4484	panupv2-all-contents-777-4484	Apps, Threats	Full	44 MB	2018/02/07 14:20:15 JST	▼	▼		リリースノート
770-4445	panupv2-all-contents-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
771-4450	panupv2-all-contents-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
775-4476	panupv2-all-contents-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
773-4465	panupv2-all-contents-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

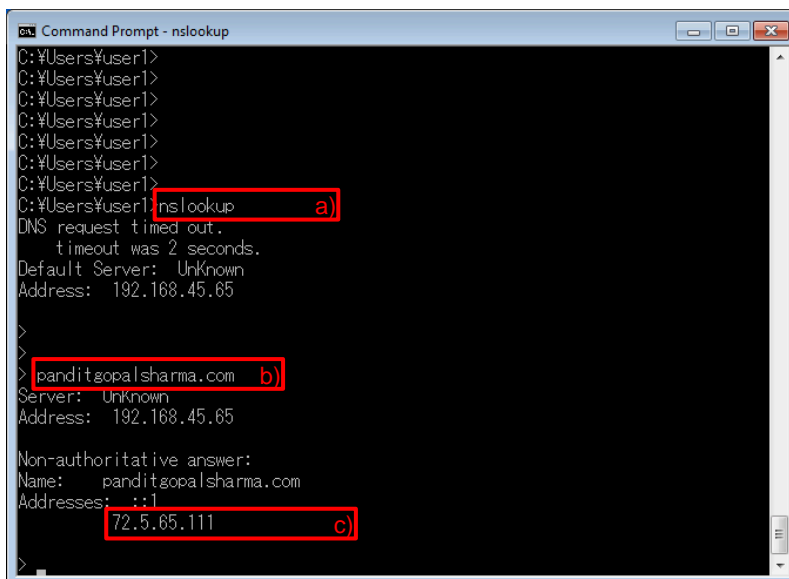
(2) リリースノート内の「New Spyware DNS C2 Signatures」でリストされているドメインのどれか一つをコピーします。

(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.dorkbot:a.najwahaifamelema43.com
generic:manavimlc.com
generic:mzykov.ru
generic:manga247.net
```

(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。



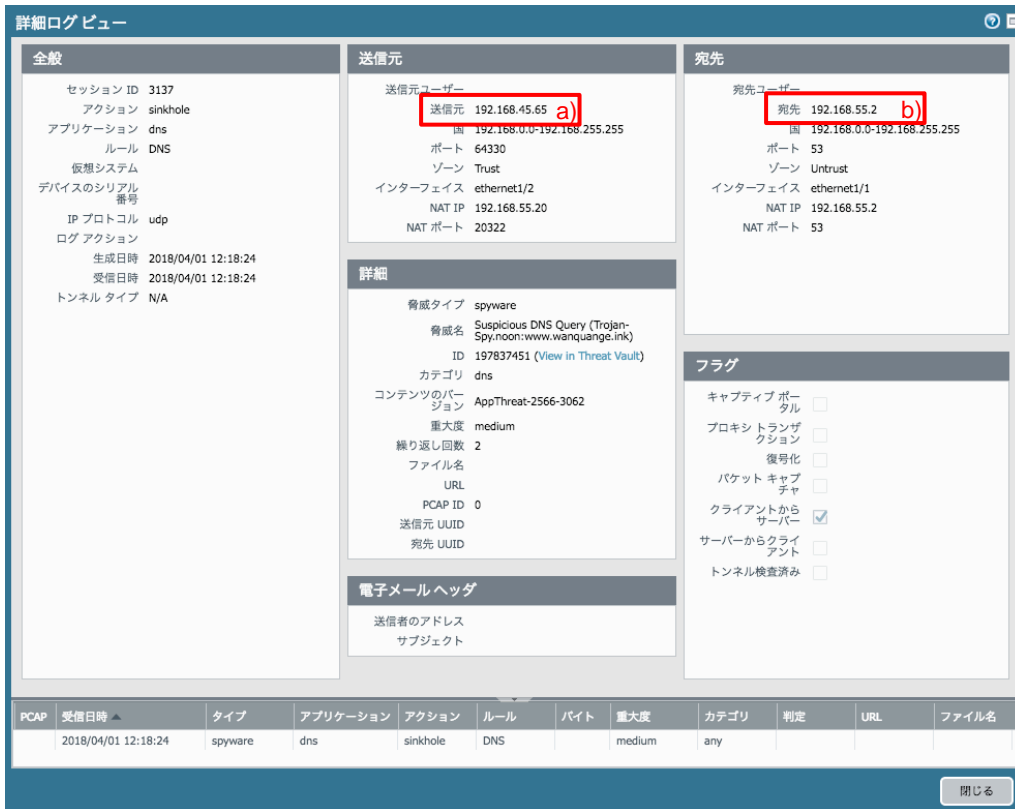
```
Command Prompt - nslookup
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1>
C:\Users\User1> nslookup
DNS request timed out.
timeout was 2 seconds.
Default Server: Unknown
Address: 192.168.45.65
>
> panditgopalsharma.com
Server: Unknown
Address: 192.168.45.65

Non-authoritative answer:
Name: panditgopalsharma.com
Addresses: ::1
72.5.65.111
```

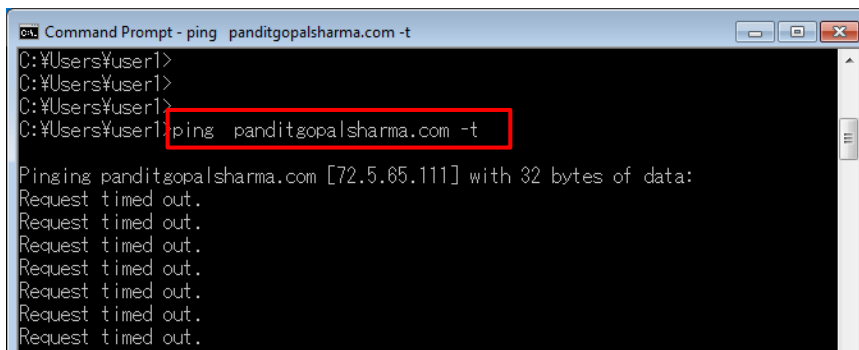
- (4) a)「Monitor」 → b)「脅威」で、タイプが「spyware」のログが出力されます。
 先頭の アイコンをクリックして、詳細ログを確認します。



- (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付きません。



- (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。)



- (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 アイコンをクリックして、詳細ログを確認します。



- (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。



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」 → b)「URL フィルタリング」 → c)「追加」をクリックします。



(2) 名前に「UF-Profile01(任意)」と入力します。



(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	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ム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其他方式で 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。



(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
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。



(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。



(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。



(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。



(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。

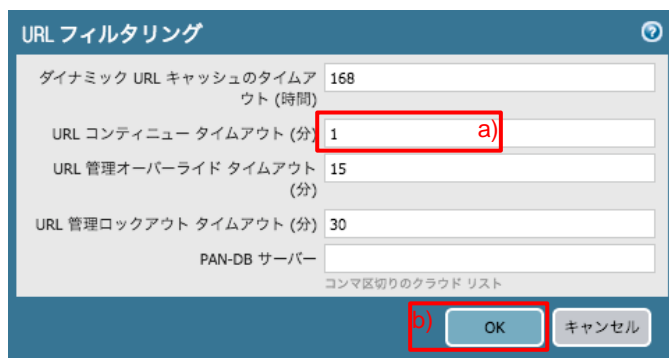


(9) デフォルトでは、一度 Continue を実施すると、15 分間は再度アクセスしても Continue 画面がでません。動作確認テスト時の 15 分は長いので、最短の 1 分に一時的に変更します。

a)「Device」 → b)「セットアップ」 → c)「コンテンツ ID」で表示された URL フィルタリングの d) ⚙️ をクリックします。



(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。



The screenshot shows a configuration window titled "URL フィルタリング" (URL Filtering). It contains several input fields for timeout settings:

- ダイナミック URL キャッシュのタイムアウト (時間): 168
- URL コンティニュー タイムアウト (分): 1 (highlighted with a red box and labeled 'a')
- URL 管理オーバーライド タイムアウト (分): 15
- URL 管理ロックアウト タイムアウト (分): 30
- PAN-DB サーバー: (empty)

At the bottom, there are two buttons: "OK" (highlighted with a red box and labeled 'b') and "キャンセル" (Cancel).

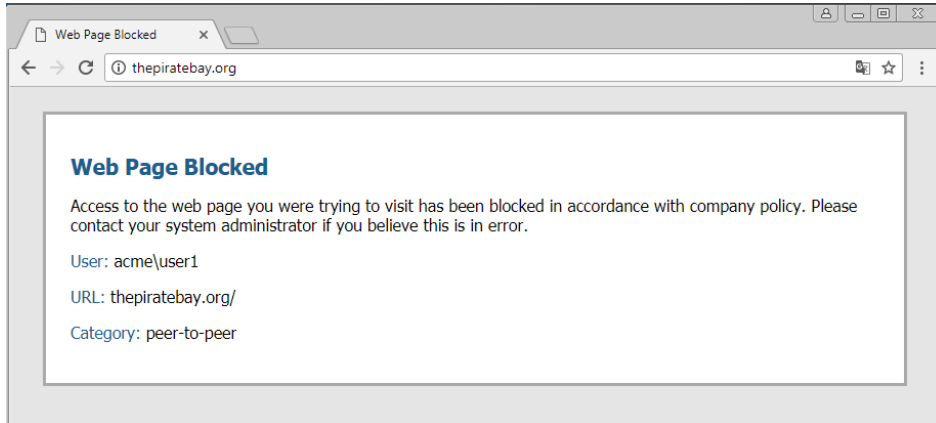
(11) 「コミット」を実施します。(方法は「設定のコミット(既述)」を参照)

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>) へアクセスします。

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。

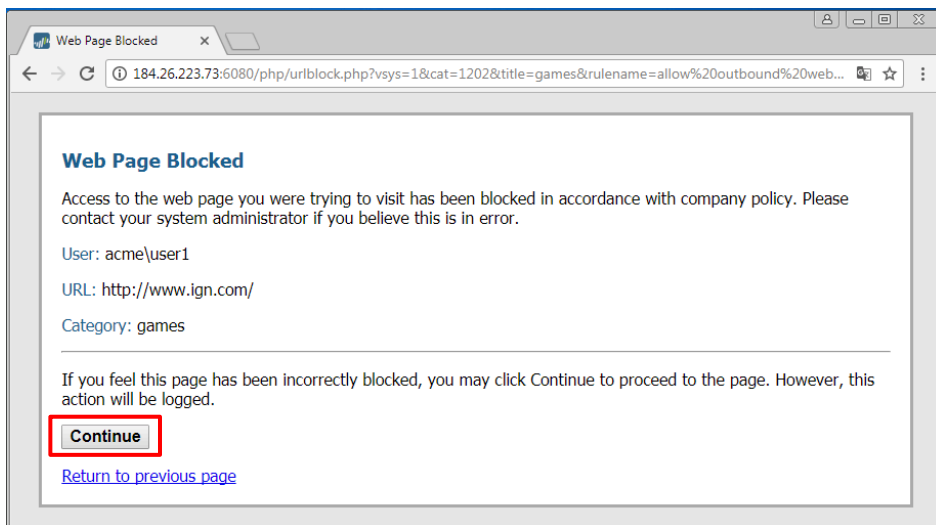
以下のように、ブロックされたことを示す画面が表示されます。



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

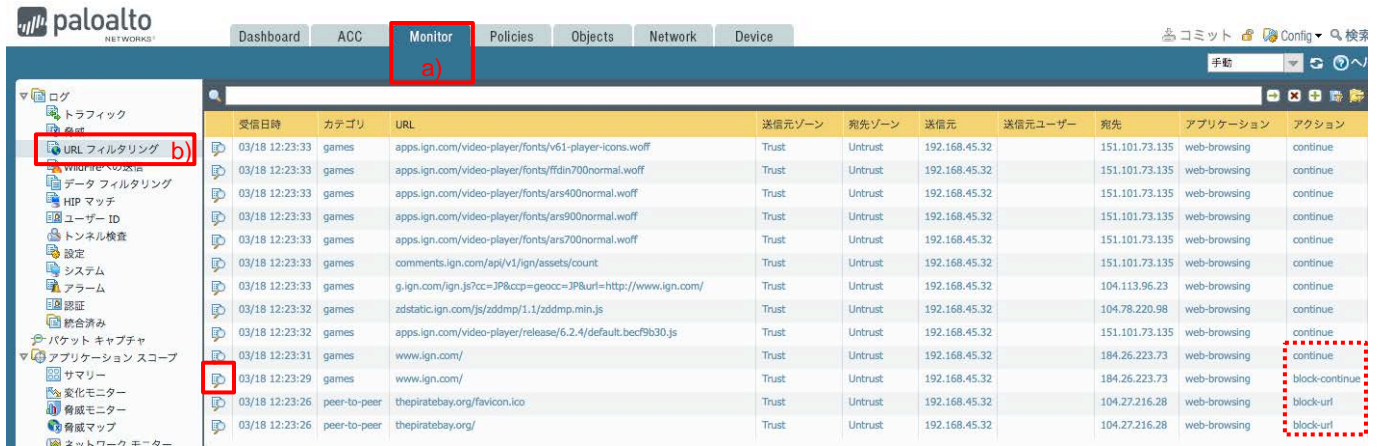
このサイトは、ビデオゲームを中心としたいくつかの娯楽に関する報道を行う Web サイトであり、Games カテゴリに属しています。

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。

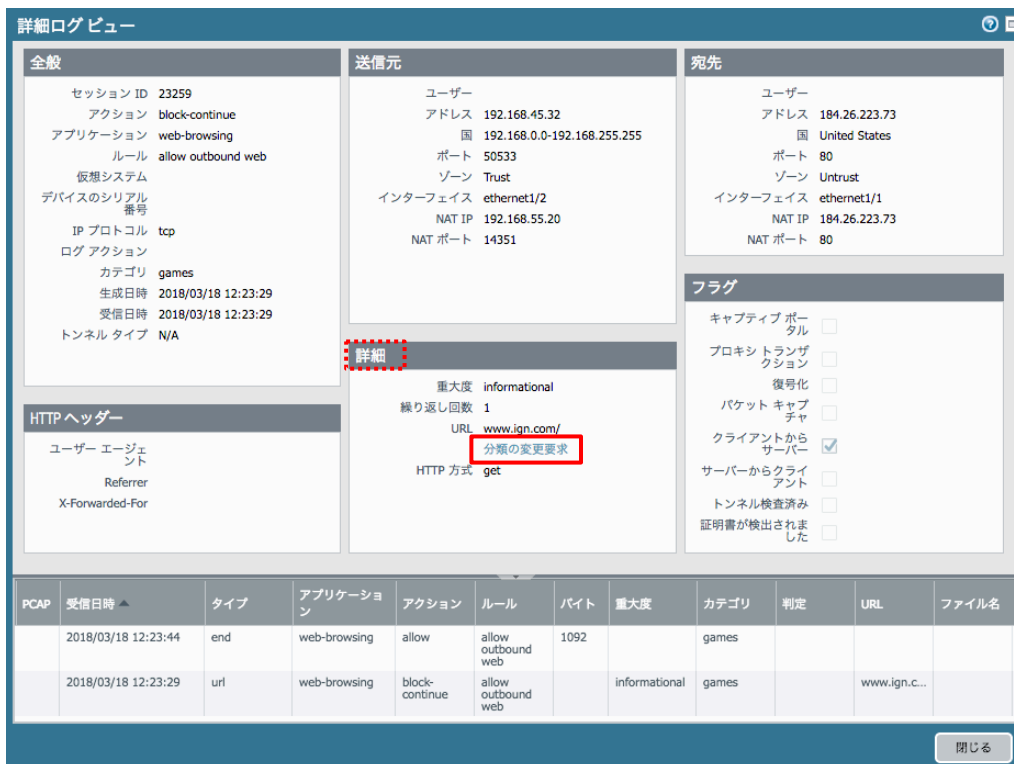


「Continue」をクリックすることで、本サイトが表示されることを確認してください。

- (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。



- (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。



- (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

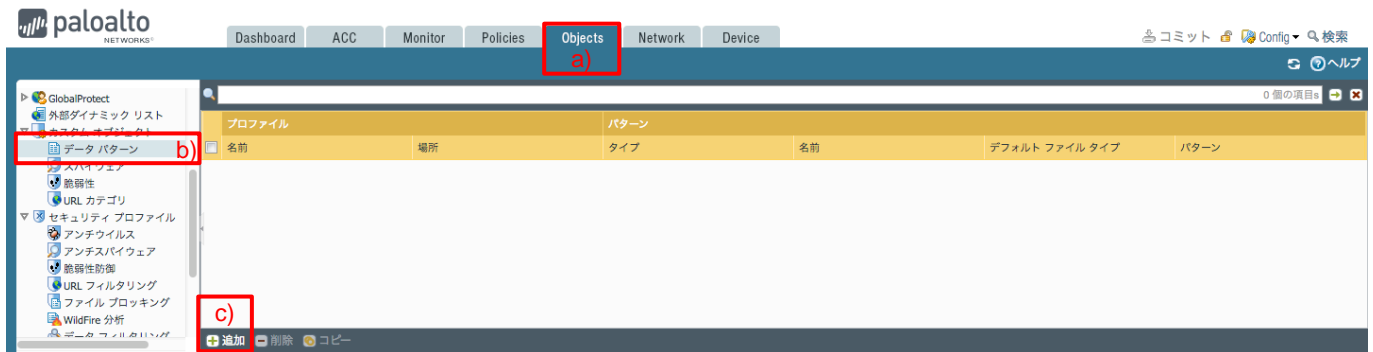
データ フィルタリングを使用すると、PA Firewall はクレジットカード番号等の機密情報を検出し、このようなデータが漏洩することを防ぐことができます。

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



(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。



(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。



- (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。



- (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。



- (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。



(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。

名前	タグ	タイプ	送信元				宛先				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
			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							
1 DNS	none	universal	Trust	any	any	any	any	Untrust	any	dns	application-default	許可		none	
2 NTP	none	universal	Trust	any	any	any	any	Untrust	any	ntp	application-default	許可			
3 Youtube-streaming	none	universal	Trust	any	any	any	any	Untrust	any	youtube-base	application-default	許可			
4 Youtube	none	universal	Trust	any	any	any	any	Untrust	any	youtube	application-default	拒否		none	
5 google-drive-web	none	universal	Trust	any	any	any	any	Untrust	any	google-drive-web	application-default	許可			
6 Risk5_file-sharing	none	universal	Trust	any	any	any	any	Untrust	any	Risk5_file-sharing	application-default	拒否		none	
7 allow outbound web	none	universal	Trust	any	any	any	any	Untrust	any	any	http	許可			
8 intrazone-default	none	intrazone	any	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	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。

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
03/18 13:47:51	online-storage-and-backup	10CC.txt		CC Number	Trust	Untrust	192.168.45.32		162.125.80.6	443	dropbox-uploading	reset-server
03/18 13:47:43	online-storage-and-backup	3CC.txt		CC Number	Trust	Untrust	192.168.45.32		162.125.80.6	443	dropbox-uploading	reset-server
03/18 13:47:33	online-storage-and-backup	3CC.txt		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

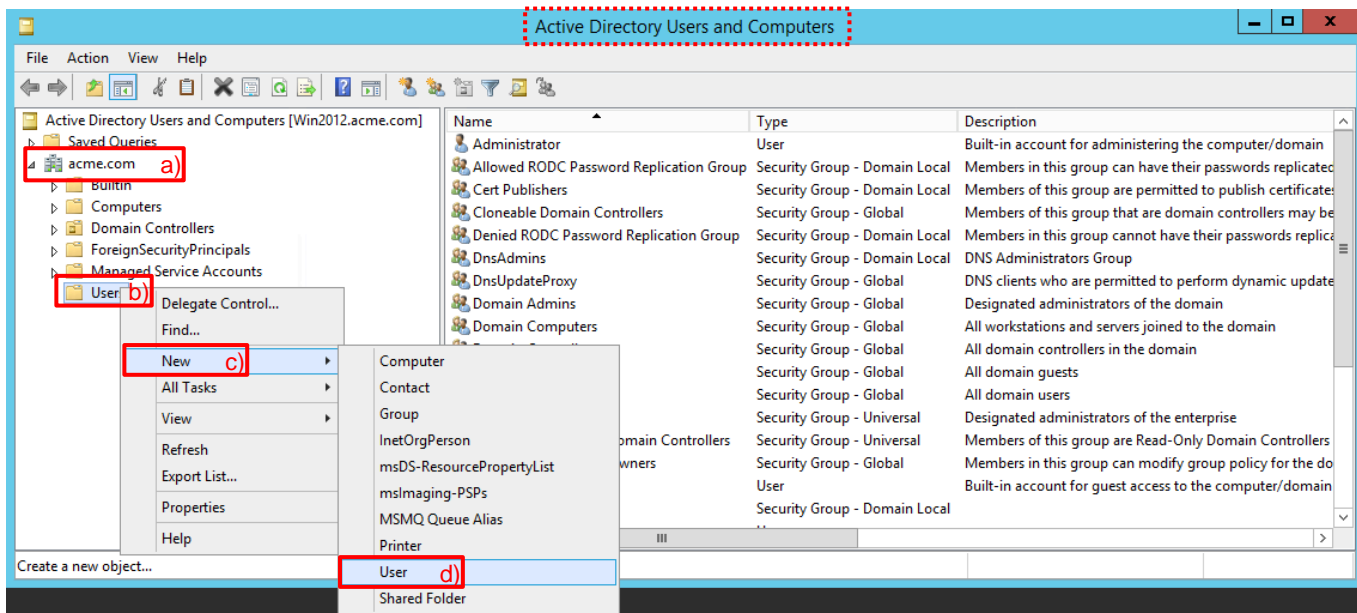
PA Firewall が AD のログを取得できるようにするための、AD 側の設定例を示します。

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。



(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

User logon name (pre-Windows 2000): ACME# panagent

< Back d) Next > Cancel

(3) a)パスワードを入力し、b)「User must change password at 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 login b)

User cannot change password

Password never expires

Account is disabled

< Back c) Next > Cancel

(4) 「Finish」をクリックします。

New Object - User

Create in: acme.com/Users

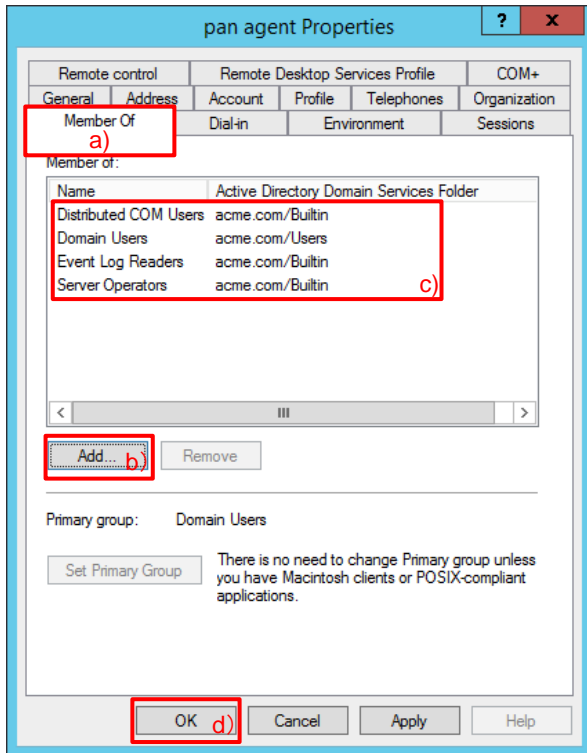
When you click Finish, the following object will be created:

Full name: pan agent

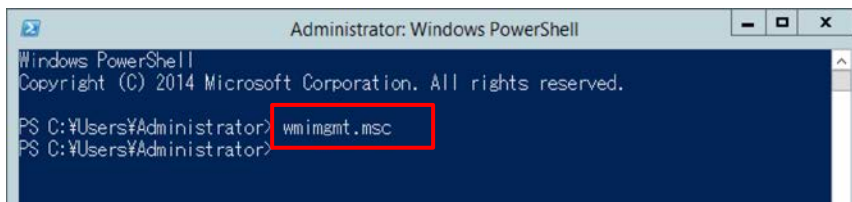
User logon name: panagent@acme.com

< Back Finish Cancel

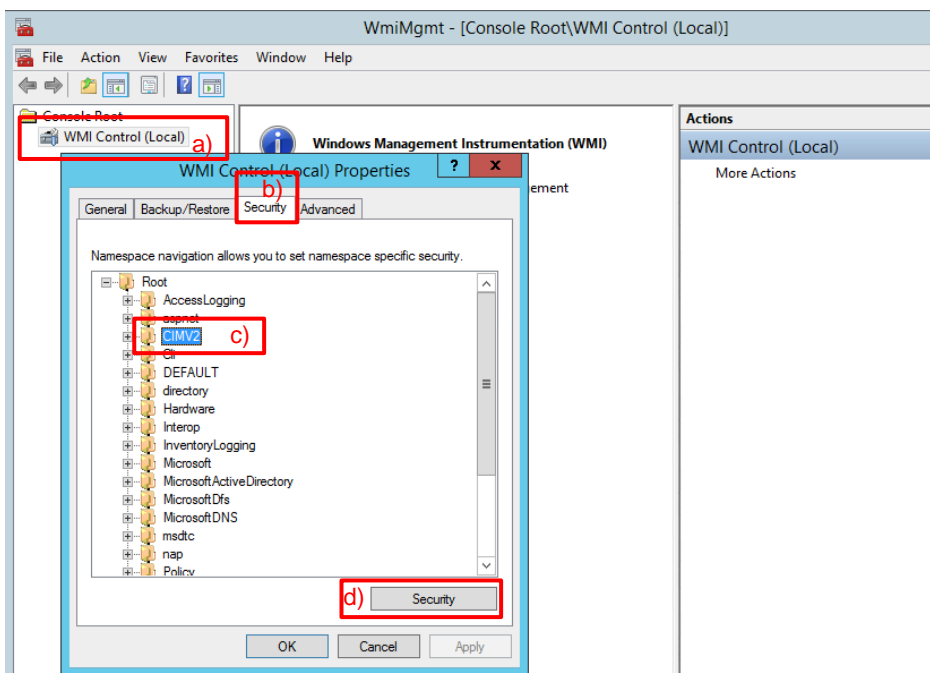
- (5) 生成した「pan agent」をダブルクリックして開き、a)「member of」タブをクリックします。
 b)「Add」をクリックして、c)3つのグループ:「Distributed COM Users」、「Event Log Readers」、「Server Operators」を付与します。d)「OK」をクリックします。



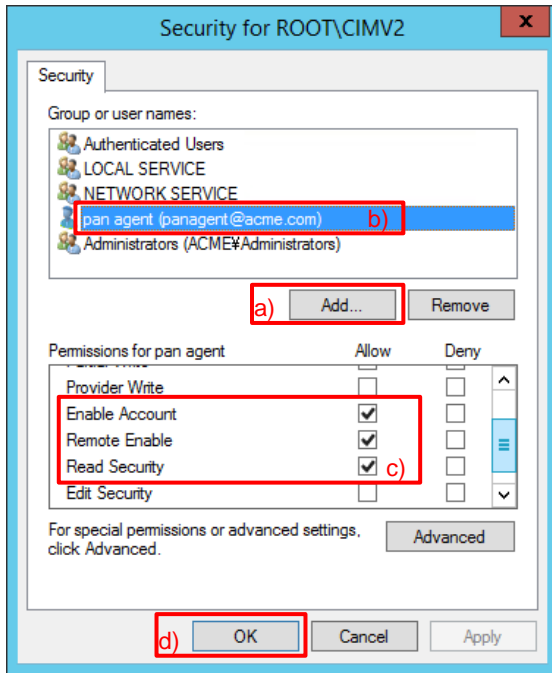
- (6) Windows PowerShell を開き、「wmimgmt.msc」と入力して Enter キーを押します。



- (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。

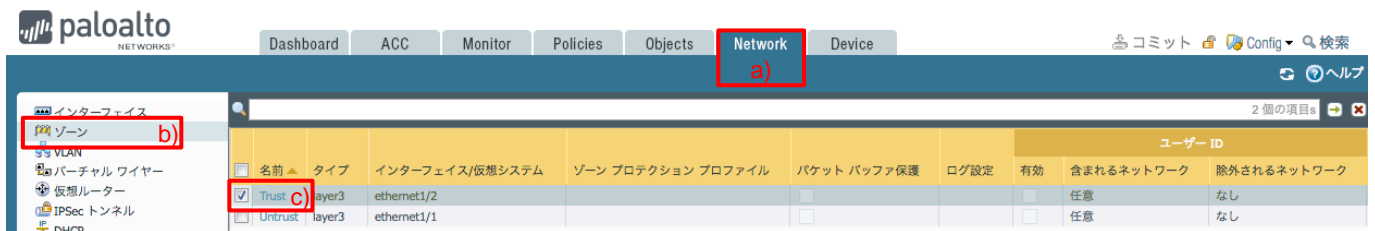


- (8) a)「Add」をクリックして、b)「pan agent」を追加します。
 c)「Pan agent」の Permissions で以下のように「Enable Account」、「Remote Enable」、「Read Security」にチェックを入れて、d)「OK」をクリックします。




13.1.2. PA Firewall の設定

- (1) a)「Network」 → b)「ゾーン」で表示された c)「Trust」をクリックします。



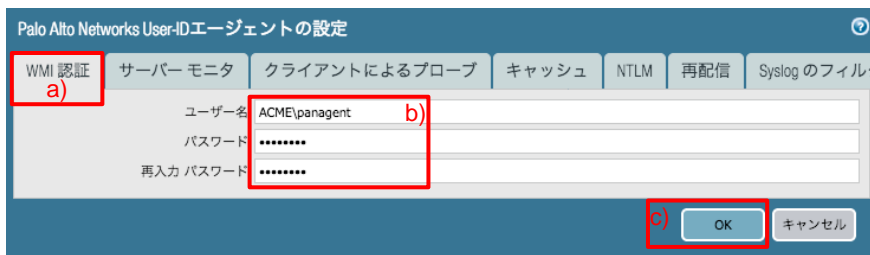
- (2) a)「ユーザ ID の有効化」にチェックを入れ、b)「OK」をクリックします。



- (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。



- (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。



- (5) a)「Device」 → b)「ユーザーID」 → 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。

- (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。

名前	有効	タイプ	ネットワーク アドレス	状態
AD	<input checked="" type="checkbox"/>	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。

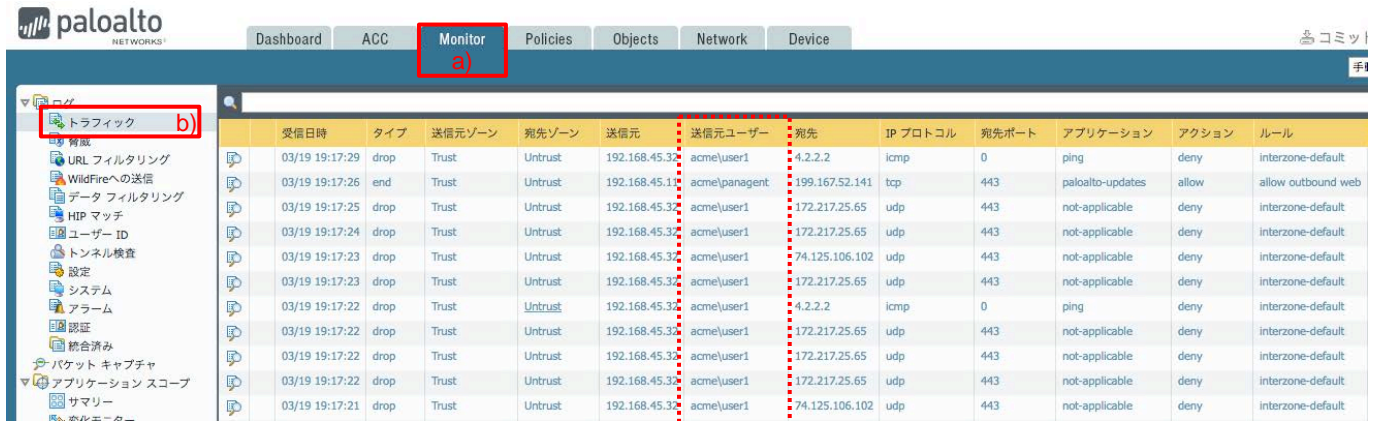
```
admin@PA-VM> show user ip-user-mapping all
```

IP	Vsys	From	User	IdleTimeout(s)	MaxTimeout(s)
192.168.45.20	vsys1	AD	acme¥panagent	1895	1895
192.168.45.32	vsys1	AD	acme¥user1	1659	1659
Total: 3 users					

- (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。



13.2.2. User-ID 連携が動作しない場合

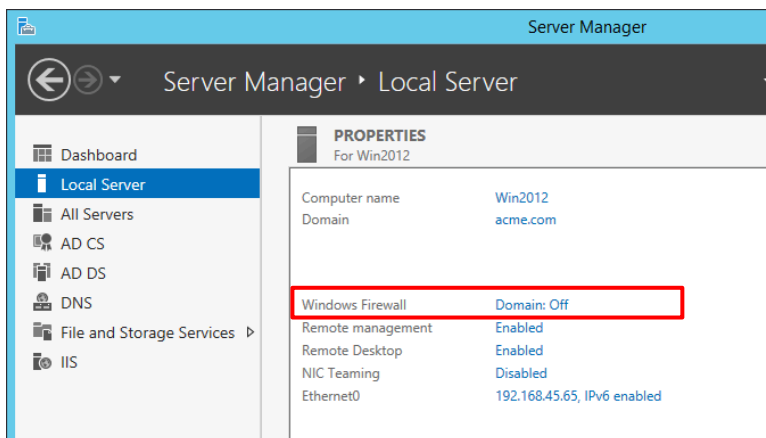
設定の見直しに加えて、以下の 2 点を確認してください。

(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。



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い合わせください。

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。

15. [参考] URL カテゴリの一覧

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.	B	C	A	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、エンジニアリング、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.	B	C	A 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 Medicine (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、治療、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 Garden (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報、製品、サービスを提供するサイト。
23			Hunting and Fishing (ハンティングとフィッシング)	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。
24		1	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。
25			Internet Communications and Telephony (インターネット通信と電話)	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たは提供するサイト。
26			Internet Portals (ポータルサイト)	通常、広範な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開始点となるサービスを提供するサイト。
27			Job Search (職探し)	求人情報や雇用評価、面接のアドバイスやヒント、雇用主と候補者の両方に対する関連サービスに関するサイト。
28			Legal (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報、分析、助言に関するサイト。
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 クラウド内の URL データベースへ問い合わせる。
35			Nudity (裸体)	作品としての性的な意図や意味があるかによらず、人体のヌードやセミヌードを含むサイト。参加者の画像を含むヌードリストやヌードリストサイトも含まれる。

No.	B	C	A	URL カテゴリ名	カテゴリ説明
36				Online Storage and Backup (オンラインストレージとバックアップ)	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。
38	1			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。
39				Personal Sites and Blogs (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。サイトが純粋なブログである場合は、" Personal Sites and Blogs " となります。
40				Philosophy and Political Advocacy (哲学と政策支援)	哲学や政治的見解に関する情報、視点やキャンペーンを含むサイト。
41	1			Phishing (フィッシング)	フィッシングやファーム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。
42				Private IP Addresses (プライベート IP アドレス)	このカテゴリには RFC1918 "Address Allocation for Private Intranets" で定義された IP アドレスを含む。 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含まれる。
43	1			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其他方式で URL フィルタリングや URL 監視をバイパスするサイト。
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サイト。
45				Real Estate (不動産)	不動産賃貸、販売、関連する助言や情報に関するサイト。不動産業者、企業、レンタルサービス、不動産情報、リフォーム関連のサイトが含まれる。
46				Recreation and Hobbies (レクリエーションと趣味)	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、および出版に関するサイト。
47				Reference and Research (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含む。
49				Search Engines (サーチエンジン)	キーワード、フレーズ、その他パラメータを使用して検索インターフェイスを提供するサイト。検索結果として情報、ウェブサイト、画像、ファイルを返す。
50				Sex Education (性教育)	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 Freeware (シェアウェアとフリーウェア)	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、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、オープンソースプ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、カタログ販売の Web サイト、価格を集約してモニタするサイトも含まれる。ここに記載されているサイトは、さまざまな商品を販売するオンライン商店、または主な目的がオンラインセールスです。オンライ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 shopping に分類される。食料品店のサイトも含まれる。

No.	B	C	A	URL カテゴリ名	カテゴリ説明
53				Social Networking (ソーシャルネットワーキング)	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 and Tools (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ア)	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 Intimate Apparel (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
59				Training and Tools (トレーニングとツール)	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 Email (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できる Web サイト。