

PA シリーズファイアウォール PPPoE Unnumbered 設定例

2018年3月 (更新)

Akira Hayashi
SE Manager, Palo Alto Networks



はじめに

PPPoE 回線を利用する際、複数のIPアドレスが割り当てられるような環境(LAN型接続)において、割り当てられたグローバルIPアドレスを直接DMZなど公開サーバに設定して使用する構成を一般にUnnumbered PPPoE 接続と呼びます。

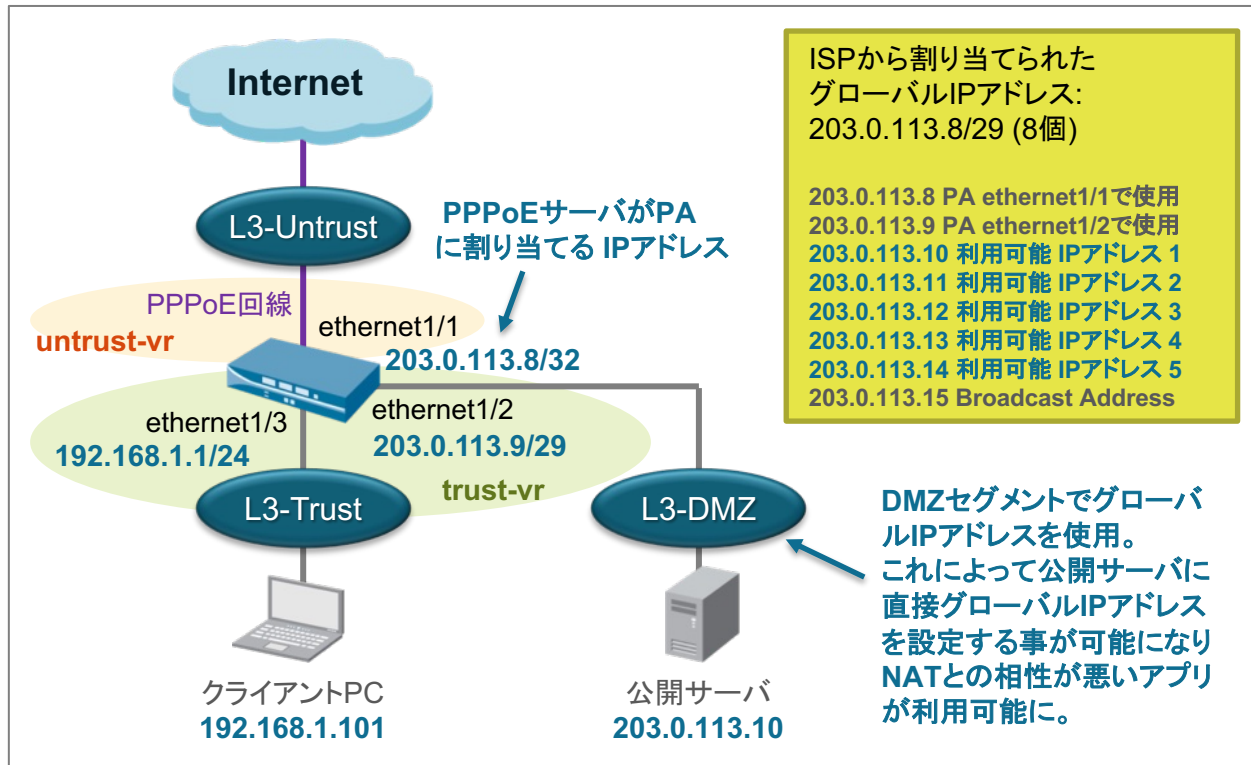
PAシリーズ次世代ファイアウォールは、複数の仮想ルータを使用することで PPPoE LAN型接続におけるグローバルIPアドレスの直接利用が可能になります。

実際の設定方法や設定・利用時のポイントは次項以降をご参照ください。

この設定例はPAN-OS 7.1 ベースですが、PAN-OS 8.0 以降でも同様の設定で動作します。

ネットワーク構成概要とPAのシステム情報

[ネットワーク構成概要]



[動作確認に使用したPAのシステム情報]

デバイス名	884-PA-VM
MGT IP アドレス	10.0.0.40
MGT ネットマスク	255.255.255.0
MGT デフォルト ゲートウェイ	10.0.0.1
MGT IPv6 アドレス	unknown
MGT IPv6 リンク ローカル アドレス	fe80::...::e55/64
MGT IPv6 デフォルト ゲートウェイ	
MGT MAC アドレス	00:0c:29:...
モデル	PA-VM
シリアル番号	0070...388
CPU ID	C206...AB1F
UUID	5640...7-EAB9-3D68-7E6F011B9E55
VM ライセンス	VM-100
VM モード	VMWare ESXi
ソフトウェア バージョン	7.1.15
GlobalProtect エージェント	4.0.6
アプリケーション バージョン	769-4439 (01/17/18)
脅威バージョン	769-4439 (01/17/18)
アンチウイルス バージョン	2498-2992 (01/21/18)
WildFire バージョン	211596-213963 (01/21/18)
URL フィルタリング バージョン	20180119.80048
GlobalProtect データファイル バージョン	1516578002 (01/22/18)
日時	Tue Jan 23 12:55:30 2018
アップ タイム	0 days, 0:42:39

※本資料ではRFC5737で規定されたドキュメント作成用に予約されたグローバルIPアドレスを使用しています。



PAのコンフィギュレーションやグローバルIPアドレス利用に関するポイント

- ✓ **PPPoE回線接続用と他のLAN I/Fに紐づけるための2つの仮想ルータを定義する**
 - **untrust-vr**: PPPoE回線に接続するI/F (ethernet1/1)
 - **trust-vr**: 内部セグメント(Trust)やDMZセグメントに接続するI/F (ethernet1/2, 1/3)
- ✓ **仮想ルータをまたぐ通信用の静的経路(Static routing)を定義する**
 - **trust-vr** には untrust-vr をnexthopとして指定したdefault route(0.0.0.0/0)を定義
 - **untrust-vr** には trust-vr をnexthopとしたDMZ及び内部ネットワーク向けの経路を定義
- ✓ **本構成で利用可能なGlobal IPアドレスは {割り当てられたGlobal IP} – {2(個)}**
 - 割り当てられた最初のIPアドレスは PPPoE回線 I/Fにアサインされ PAT用として使用
 - 2個目以降のIPアドレスは最後のBroadcast Addressを除き、自由に利用可能
 - 例1: IP8プランの場合、5個のGlobal IPアドレス、1個のN対1 NAT用 IPアドレス
 - 例2: IP16プランの場合、13個のGlobal IPアドレス、1個のN対1 NAT用 IPアドレス

PAの設定： インターフェイス, ゾーン設定 (Network > インターフェイス, ゾーン)

[インターフェイス一覧] *特別な定義は不要

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	セキュリティ ゾーン	機能
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	untrust-vr	Untagged	L3-Untrust	
ethernet1/2	Layer3	ping-only		203.0.113.9/29	trust-vr	Untagged	L3-DMZ	DNS ✓
ethernet1/3	Layer3	PA-mgmt		192.168.1.1/24	trust-vr	Untagged	L3-Trust	IP ✓ DNS ✓

[ゾーン一覧] *特別な定義は不要

名前	タイプ	インターフェイス/仮想システム
L3-Untrust	layer3	ethernet1/1
L3-Trust	layer3	ethernet1/3
L3-DMZ	layer3	ethernet1/2

ISPから発行されたPPPoEユーザ名とパスワードを入力

スタティックアドレスはGlobalProtectを使用する場合を除き、無指定(Noneのまま)が良い

NTTフレッツ系回線の場合MTUは1454を指定

PAの設定： 仮想ルータ設定 (Network > 仮想ルーター)

[仮想ルーター一覧]

名前	インターフェイス	設定	ランタイム状態
trust-vr	ethernet1/2	スタティック ルート: 1	詳細ランタイム状態
	ethernet1/3	ECMP の状態: 無効	
untrust-vr	ethernet1/1	スタティック ルート: 2	詳細ランタイム状態
		ECMP の状態: 無効	

[実際の経路情報(trust-vr)]

宛先	ネクスト ホップ	メトリック	フラグ	インターフェイス
0.0.0.0/0	vr untrust-vr	10	A S	trust-vr0
192.168.1.0/24	vr trust-vr	10	A S	ethernet1/3
192.168.1.1	vr trust-vr	0	A C	ethernet1/3
192.168.1.32	vr trust-vr	0	A H	ethernet1/3
203.0.113.0/24	vr trust-vr	0	A C	ethernet1/2
203.0.113.32	vr trust-vr	0	A H	ethernet1/2

[実際の経路情報(untrust-vr)]

宛先	ネクスト ホップ	メトリック	フラグ	インターフェイス
0.0.0.0/0	vr trust-vr	10	A S	ethernet1/1
192.168.1.0/24	vr trust-vr	10	A S	ethernet1/1
192.168.1.1	vr trust-vr	0	A S	ethernet1/1
192.168.1.32	vr trust-vr	0	A S	ethernet1/1
203.0.113.0/24	vr trust-vr	10	A S	ethernet1/2
203.0.113.32	vr trust-vr	0	A H	ethernet1/2

[PPPoE回線側仮想ルーター “untrust-vr” 設定]

trust-vr をNexthopにしたDMZ及び内部ネットワーク IPサブネット向けのスタティックルートを設定

[その他のLAN (DMZ, 内部) I/F用 仮想ルーター “trust-vr” 設定]

untrust-vr をNexthopにしたデフォルトルートを設定



PAの設定：セキュリティ, NATポリシー設定 (Policies > セキュリティ, NAT)

[セキュリティポリシー] *特別な定義は不要

名前	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	ゾーン	アドレス					
1 Trust-to-Untrust	universal	L3-Trust	any	any	L3-Untrust	any	any	application-default	許可	none	
2 Trust-to-DMZ	universal	L3-Trust	any	any	L3-DMZ	any	any	application-default	許可	none	
3 Untrust-to-DMZ	universal	L3-Untrust	any	any	L3-DMZ	any	any	application-default	許可	none	
4 DMZ-to-Untrust	universal	L3-DMZ	any	any	L3-Untrust	any	any	application-default	許可	none	
5 intrazone-default	intrazone	any	any	any	(intrazone)	any	any	any	許可	none	none
6 interzone-default	interzone	any	any	any	any	any	any	any	拒否	none	none

実際の環境に合わせて設定を変更すること

[NATポリシー] *特別な定義は不要

名前	タグ	元のバケット							変換済みバケット	
		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 N to 1 NAT	none	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none	

ISPから割り当てられた
グローバルIPアドレス:
203.0.113.8/29 (8個)

203.0.113.8 PA ethernet1/1で使用
203.0.113.9 PA ethernet1/2で使用
203.0.113.10 利用可能 IPアドレス 1
203.0.113.11 利用可能 IPアドレス 2
203.0.113.12 利用可能 IPアドレス 3
203.0.113.13 利用可能 IPアドレス 4
203.0.113.14 利用可能 IPアドレス 5
203.0.113.15 Broadcast Address

内部ネットワークのクライアントがインターネットに通信する際、送信元IPアドレスはPAのethernet1/1に割り当てられたIPアドレスにNAT変換される



PPPoE 回線接続状態の表示 :

[Web UIの場合]

ダイナミック IP インターフェイス状態

Interface	ethernet1/1
Local IP Address	203.0.113.8
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Remote IP Address	198.51.100.254
PPPoE State	Connected
PPP State	Connected
Access Concentrator	PANW-Lab-PPPoE-Server
AC MAC	00:11:11:11:11:b9
Authentication Method	CHAP
Passive mode	Disabled
Link MTU	1454

接続 閉じる

リンク状態	IP アドレス	仮想ルーター
	Dynamic-PPPoE	untrust-vr
	203.0.113.9/29	trust-vr
	192.168.1.1/24	trust-vr

ここをクリック！

[CLIの場合]

```
ahayashi@PA> show pppoe interface ethernet1/1
```

```
Interface: ethernet1/1
PPPoE State: Connected
PPP State: Connected
Connected since: Tue Jan 23 12:17:17 2018
Connection up for: 49709 days, 8:08:56
Access Concentrator: PANW-Lab-PPPoE-Server
AC MAC: 00:11:11:11:11:b9
Authentication via: CHAP
Passive mode: Disabled
Username: pppoe-user01
Local IP: 203.0.113.8
Primary DNS IP: 8.8.8.8
Secondary DNS IP: 8.8.4.4
Primary WINS IP: 0.0.0.0
Secondary WINS IP: 0.0.0.0
Remote IP: 198.51.100.254
Session ID: 30
Link MTU: 1454
PPPoE/PPP Counters:
PPPoE control packets received: 2
PPPoE control packets sent: 2
PPP control packets received: 1918
PPP control packets sent: 1918
```



トラフィックログ例： Untrust (PPPoE回線) → DMZ (Global IP)

[トラフィック詳細ログ] *Global IPアドレスを設定したDMZセグメント上の公開サーバへアクセス

詳細ログビュー

全般	送信元	宛先
セッション ID 120 アクション allow アクションの送信元 from-policy アプリケーション ssl ルール Untrust-to-DMZ セッション終了理由 tcp-rst-from-client カテゴリ any 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 2018/01/23 12:27:05 開始時間 2018/01/23 12:26:50 受信日時 2018/01/23 12:27:05 経過時間 (秒) 0	ユーザー アドレス 198.51.100.254 国 198.51.100.0-198.51.100.255 ポート 58984 ゾーン L3-Untrust インターフェイス ethernet1/1	ユーザー アドレス 203.0.113.10 国 203.0.113.0-203.0.113.255 ポート 443 ゾーン L3-DMZ インターフェイス ethernet1/2
	詳細	フラグ
	バイト 4216 受信済みバイト 2999 送信済みバイト 1217 繰り返し回数 1 パケット 17 受信したパケット 8 送信したパケット 9	キャプティブ ポータル <input type="checkbox"/> プロキシ トランザクション <input type="checkbox"/> 復号化 <input type="checkbox"/> パケット キャプチャ <input type="checkbox"/> クライアントからサーバー <input type="checkbox"/> サーバーからクライアント <input type="checkbox"/> 対称リターン <input type="checkbox"/> ミラーリング済み <input type="checkbox"/>

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	カテゴリ
	2018/01/23 12:27:05	end	ssl	allow	Untrust-to-DMZ	4216	any

閉じる

Global IPアドレスが設定されたDMZセグメント上のサーバに対しNAT処理なしにダイレクトに通信が行われている

トラフィックログ例： DMZ (Global IP) → Untrust (PPPoE回線)

[トラフィック詳細ログ]

詳細ログビュー

全般	送信元	宛先
セッション ID 4426 アクション allow アクションの送信元 from-policy アプリケーション yum ルール DMZ-to-Untrust セッション終了理由 tcp-fin カテゴリ business-and-economy 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 2018/01/23 11:54:11 開始時間 2018/01/23 11:53:57 受信日時 2018/01/23 11:54:11 経過時間 (秒) 0	ユーザー アドレス 172.16.1.10 国 172.16.0.0-172.31.255.255 ポート 47568 ゾーン L3-DMZ インターフェイス ethernet1/2	ユーザー アドレス 202.232.140.70 国 Japan ポート 80 ゾーン L3-Untrust インターフェイス ethernet1/1
	詳細	フラグ
	バイト 4852 受信済みバイト 4236 送信済みバイト 616 繰り返し回数 1 パケット 14 受信したパケット 7 送信したパケット 7	キャプティブ ポータル <input type="checkbox"/> プロキシ トランザクション <input type="checkbox"/> 復号化 <input type="checkbox"/> パケット キャプチャ <input type="checkbox"/> クライアントからサーバー <input type="checkbox"/> サーバーからクライアント <input type="checkbox"/> 対称リターン <input type="checkbox"/> ミラーリング済み <input type="checkbox"/>

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	カテゴリ
	2018/01/23 11:54:11	end	yum	allow	DMZ-to-Untrust	4852	business-and-economy

閉じる

DMZセグメント上のサーバからインターネットに対しNAT処理なしにダイレクトに通信が行われている

トラフィックログ例：内部セグメント (Trust) → Untrust (PPPoE回線)

[トラフィック詳細ログ]

詳細ログビュー

全般	送信元	宛先
セッション ID 393 アクション allow アクションの送信元 from-policy アプリケーション ms-office365-base ルール Trust-to-Untrust セッション終了理由 tcp-fin カテゴリ computer-and-internet-info 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	ユーザー アドレス 192.168.1.101 国 192.168.0.0-192.168.255.255 ポート 49623 ゾーン L3-Trust インターフェイス ethernet1/3 NAT IP 203.0.113.8 NAT ポート 61910	ユーザー アドレス 23.100.101.120 国 Japan ポート 443 ゾーン L3-Untrust インターフェイス ethernet1/1 NAT IP 23.100.101.120 NAT ポート 443
生成日時 2018/01/23 14:17:53 開始時間 2018/01/23 14:15:49 受信日時 2018/01/23 14:17:53 経過時間 (秒) 110	詳細 バイト 11454 受信済みバイト 7878 送信済みバイト 3576 繰り返し回数 1 パケット 24 受信したパケット 10 送信したパケット 14	フラグ キャプティブポータル <input type="checkbox"/> プロキシトランザクション <input type="checkbox"/> 復号化 <input type="checkbox"/> パケットキャプチャ <input type="checkbox"/> クライアントからサーバー <input type="checkbox"/> サーバーからクライアント <input type="checkbox"/> 対称リターン <input type="checkbox"/> ミラーリング済み <input type="checkbox"/>

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	カテゴリ
	2018/01/23 14:17:53	end	ms-office365-base	allow	Trust-to-Untrust	11454	computer-and-internet-info

閉じる



トラフィックログ例：内部セグメント (Trust) → DMZ (Global IP)

[トラフィック詳細ログ]

詳細ログビュー

全般	送信元	宛先
セッション ID 425 アクション allow アクションの送信元 from-policy アプリケーション ssl ルール Trust-to-DMZ セッション終了理由 tcp-rst-from-client カテゴリ any 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 2018/01/23 14:26:35 開始時間 2018/01/23 14:26:20 受信日時 2018/01/23 14:26:35 経過時間 (秒) 0	ユーザー アドレス 192.168.1.101 国 192.168.0.0-192.168.255.255 ポート 49637 ゾーン L3-Trust インターフェイス ethernet1/3	ユーザー アドレス 203.0.113.10 国 203.0.113.0-203.0.113.255 ポート 443 ゾーン L3-DMZ インターフェイス ethernet1/2
	詳細	フラグ
	バイト 2782 受信済みバイト 1966 送信済みバイト 816 繰り返し回数 1 パケット 14 受信したパケット 6 送信したパケット 8	キャプティブポート <input type="checkbox"/> プロキシトランザクション <input type="checkbox"/> 復号化 <input type="checkbox"/> パケットキャプチャ <input type="checkbox"/> クライアントからサーバー <input type="checkbox"/> サーバーからクライアント <input type="checkbox"/> 対称リターン <input type="checkbox"/> ミラーリング済み <input type="checkbox"/>

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	カテゴリ
	2018/01/23 14:26:35	end	ssl	allow	Trust-to-DMZ	2782	any

閉じる



THANK YOU

Email: ahayashi@paloaltonetworks.com | Twitter: @PaloAltoNtwks

