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。

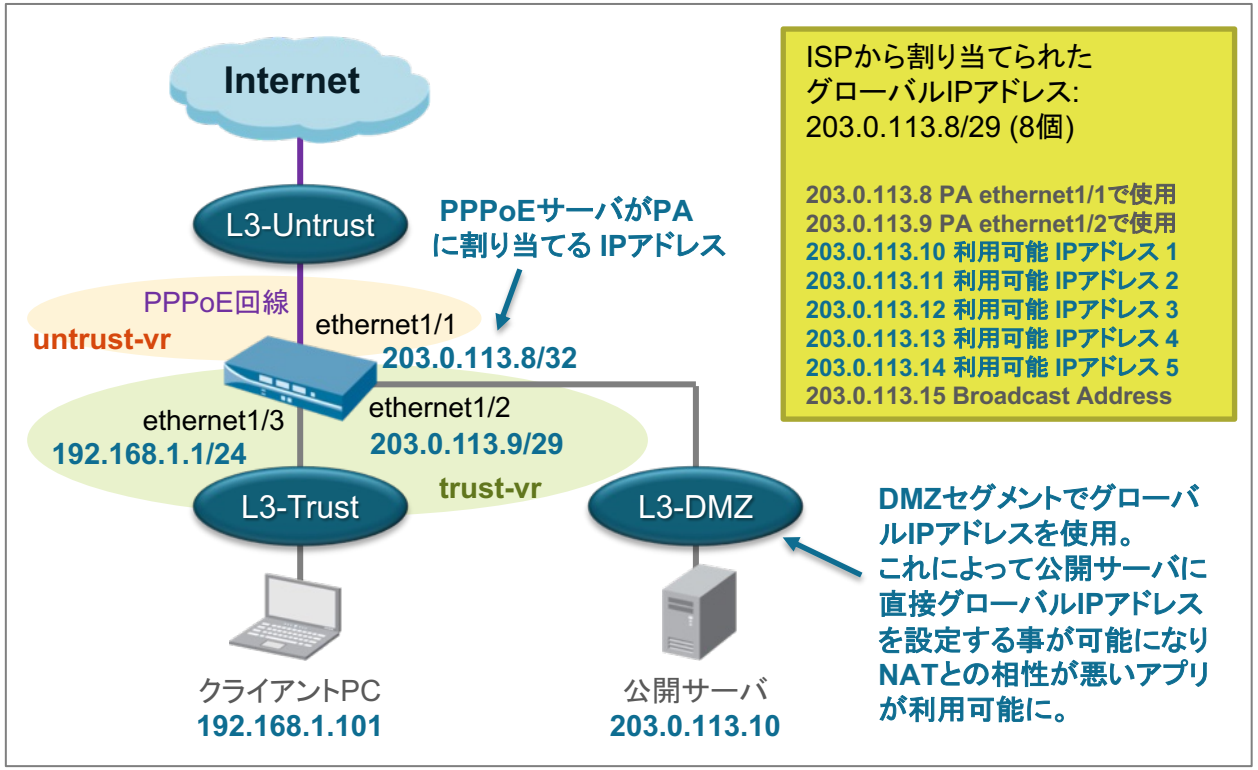
実際の設定方法や設定・利用時のポイントは次項以降をご参照ください。

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。

 © 2018, Palo Alto Networks. Confidential and Proprietary.

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 .40
MGT ネットマスク	2 .0
MGT デフォルト ゲートウェイ	1 4.1
MGT IPv6 アドレス	unknown
MGT IPv6 リンク ローカル アドレス	fe80: le55/64
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。

 © 2018, Palo Alto Networks. Confidential and Proprietary.

PAのコンフィグ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

 © 2018, Palo Alto Networks. Confidential and Proprietary.

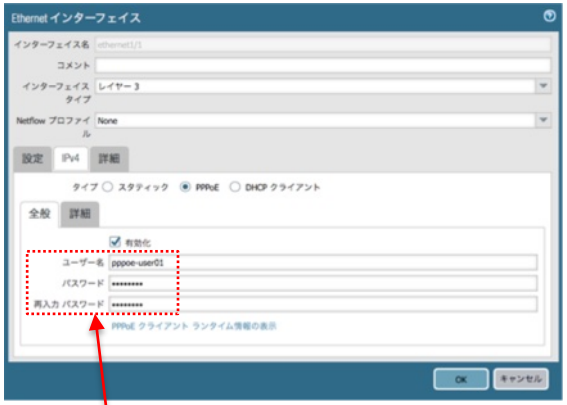
PAの設定： インターフェイス, ゾーン設定 (Network > インターフェイス, ゾーン)

[インターフェイス一覧] *特別な定義は不要

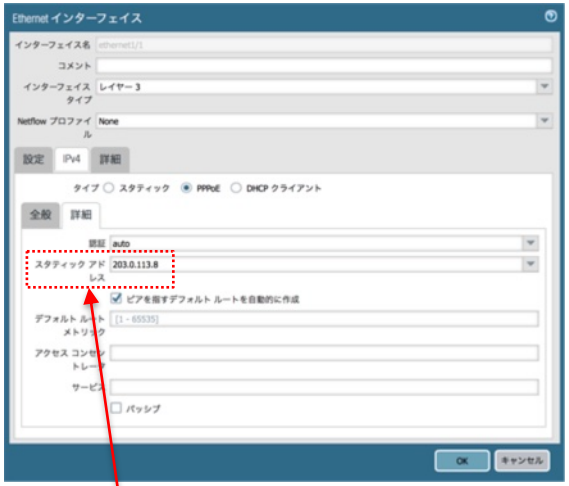
インターフェイス	インターフェイス タイプ	管理プロファイル	リンク状態	IP アドレス	仮想ルーター	タグ	セキュリティ ゾーン	機能
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	untrust-vr	Untagged	L3-Untrust	
ethernet1/2	Layer3	ping-only		203.0.113.9/29	trust-vr	Untagged	L3-DMZ	DNS
ethernet1/3	Layer3	PA-mgmt		192.168.1.1/24	trust-vr	Untagged	L3-Trust	IP DNS

[ゾーン一覧] *特別な定義は不要

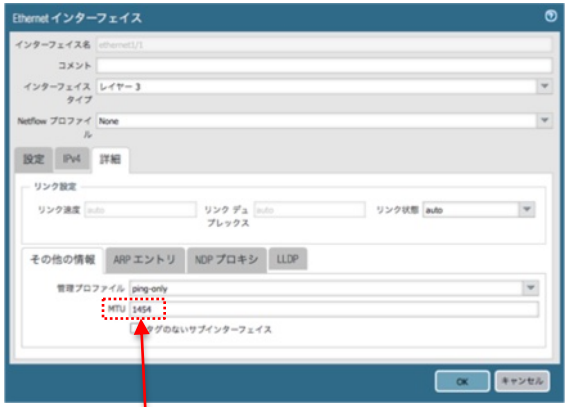
	名前	タイプ	インターフェイス/仮想システム
	L3-Untrust	layer3	ethernet1/1
	L3-Trust	layer3	ethernet1/3
	L3-DMZ	layer3	ethernet1/2



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)で良い



NTTフレッツ系回線の場合MTUは1454を指定

 © 2018, Palo Alto Networks. Confidential and Proprietary.

PAの設定： 仮想ルータ設定 (Network > 仮想ルーター)

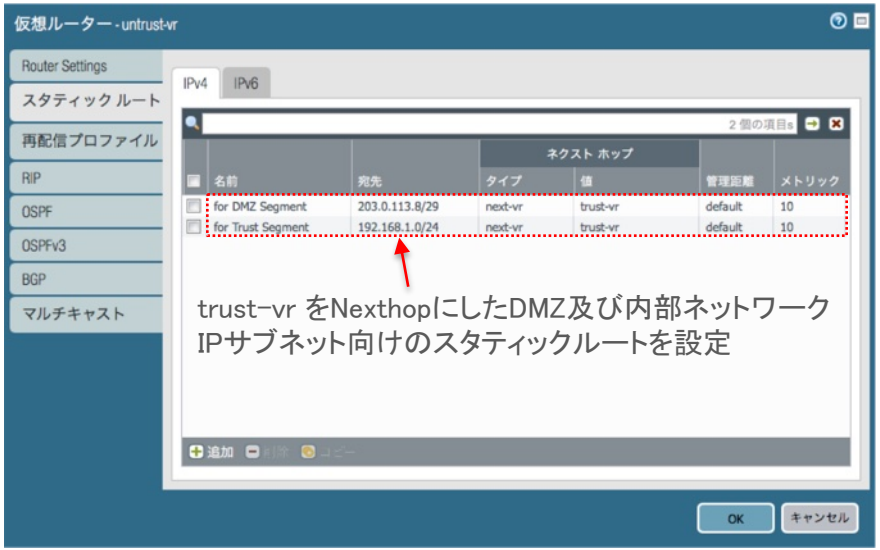
[仮想ルーター一覧]

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	詳細ランライム状態
	ethernet1/3	ECMP の状態: 無効	
untrust-vr	ethernet1/1	スタティック ルート: 2	詳細ランライム状態
		ECMP の状態: 無効	

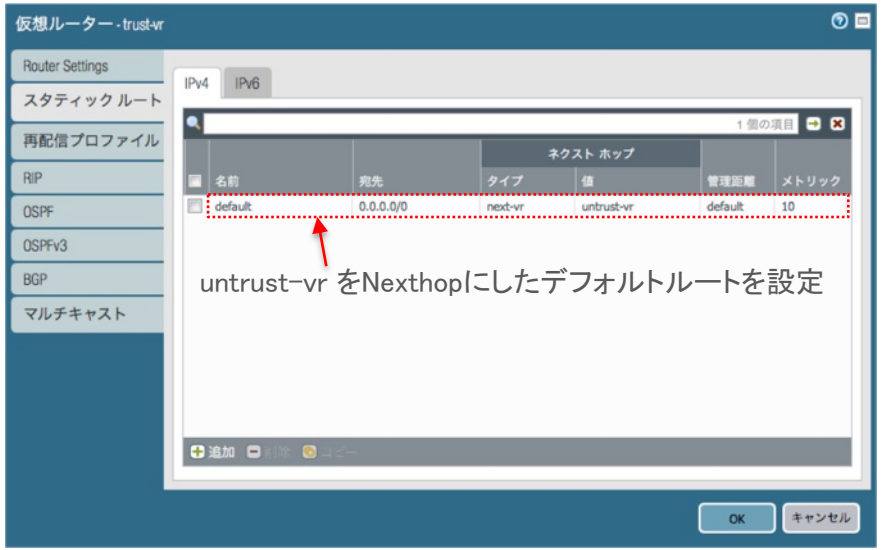
[実際の経路情報(trust-vr)]

[実際の経路情報(untrust-vr)]

[PPPoE回線側仮想ルーター “untrust-vr” 設定]



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



 © 2018, Palo Alto Networks. Confidential and Proprietary.

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	元のパケット						変換済みパケット	
			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)

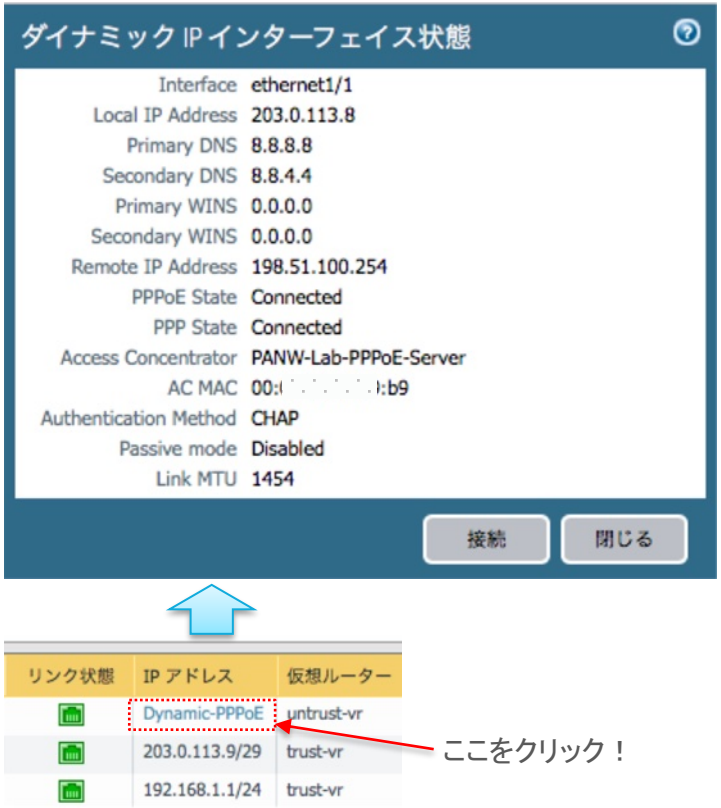
203.0.113.8 PA ethernet1/1で使用
203.0.113.9 PA ethernet1/2で使用
203.0.113.10 利用可能 IPアドレス 1
203.0.113.11 利用可能 IPアドレス 2
203.0.113.12 利用可能 IPアドレス 3
203.0.113.13 利用可能 IPアドレス 4
203.0.113.14 利用可能 IPアドレス 5
203.0.113.15 Broadcast Address

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

 © 2018, Palo Alto Networks. Confidential and Proprietary.

PPPoE 回線接続状態の表示：

[Web UIの場合]



[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:**:**:9f:b9: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
```

 © 2018, Palo Alto Networks. Confidential and Proprietary.

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

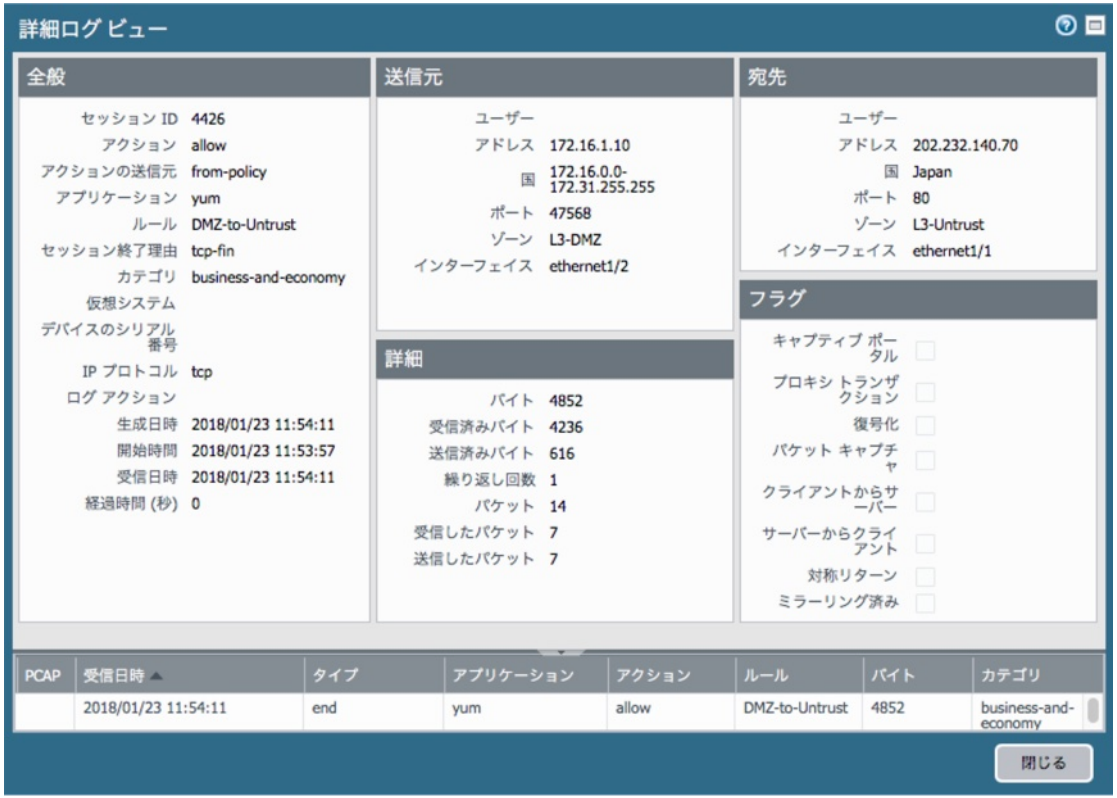
[トラフィック詳細ログ] *Global IPアドレスを設定したDMZセグメント上の公開サーバへアクセス

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

 © 2018, Palo Alto Networks. Confidential and Proprietary.

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]

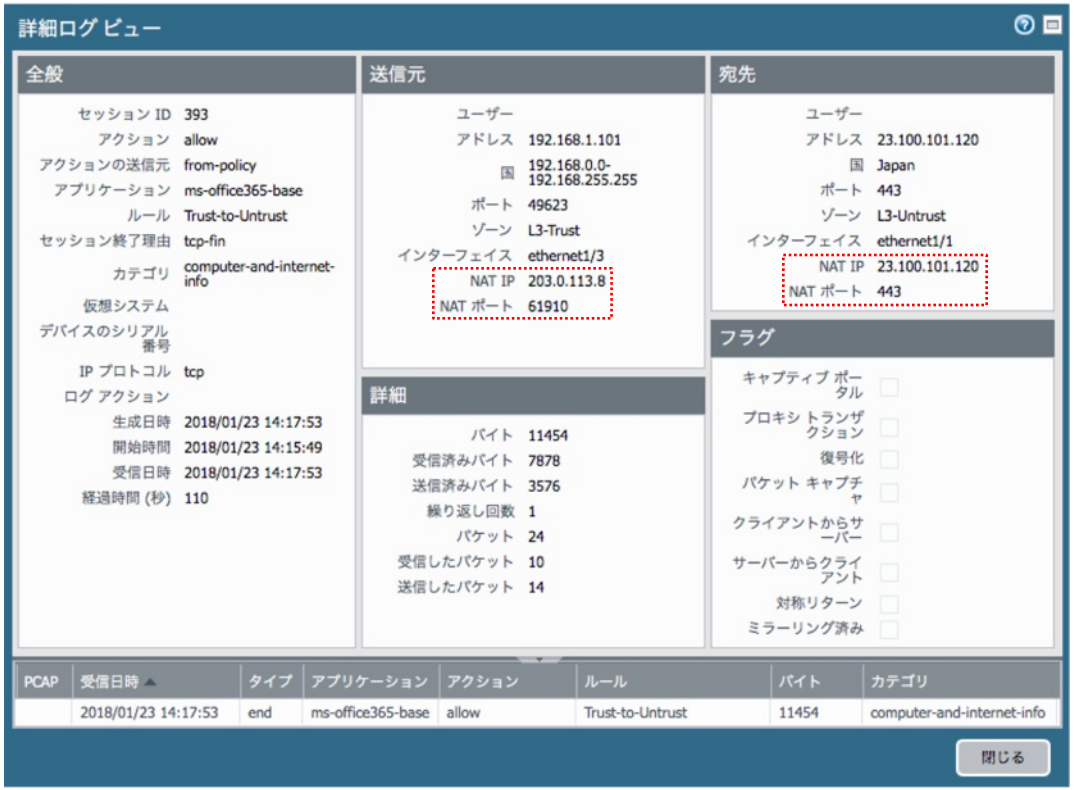


DMZセグメント上のサーバから
インターネットに対しNAT処理なしに
ダイレクトに通信が行われている

 © 2018, Palo Alto Networks. Confidential and Proprietary.

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

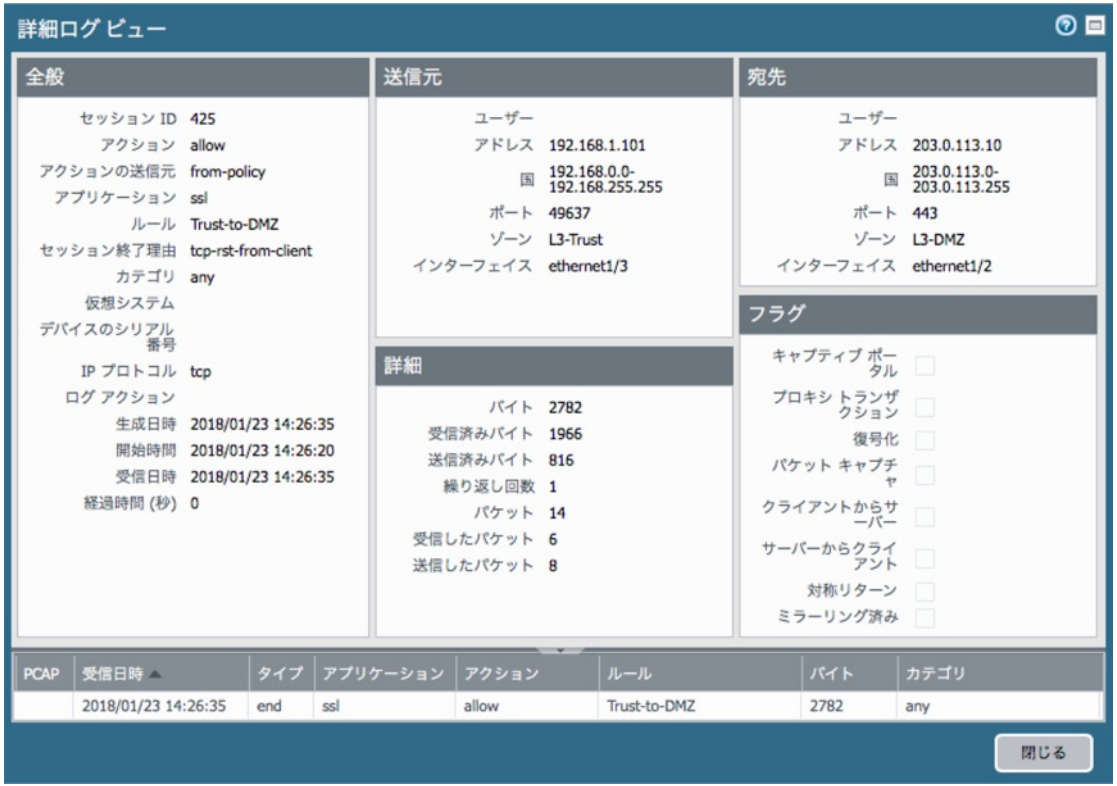
[トラフィック詳細ログ]



 © 2018, Palo Alto Networks. Confidential and Proprietary.

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]



 © 2018, Palo Alto Networks. Confidential and Proprietary.

THANK YOU

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