PA シリーズファイアウォール
PPPoE クイックコンフィグレーションガイド

March, 2018

Akira Hayashi
SE Manager - Japan

paloalto NETWORKS®

はじめに

このドキュメントは、PAシリーズファイアウォールを PPPoE 回線と共に使用する構成において、設定方法の学習・設計・検証の効率化とミスの削減を主な目的として作成されました。

このドキュメントに記載のコンフィグレーション方法と、PAシリーズファイアウォール中核機能である**脅威防御関連設定**を組み合わせ PAシリーズファイアウォールを展開することで、比較的セキュリティレベルが低く、近年サイバー攻撃の進入口として狙われやすいブランチオフィス等の小規模拠点におけるセキュリティレベルを飛躍的に向上させることが可能になります。

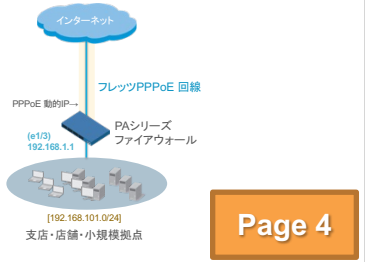
本資料を弊社Webサイトの製品ドキュメントと共にご活用下さい。

<製品ドキュメントページ>
https://www.paloaltonetworks.com/documentation

<PAN-OS 7.1関連日本語マニュアル>
https://www.paloaltonetworks.com/documentation/translated/71

このドキュメントでカバーしている**PPPoE** 設定構成

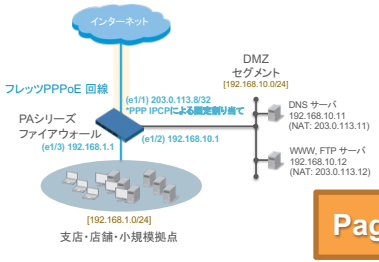
設定例 1



Page 4

最もベーシックな接続構成

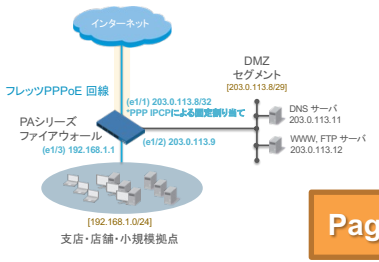
設定例 2



Page 21

公開サーバの保護1 (DMZあり構成)

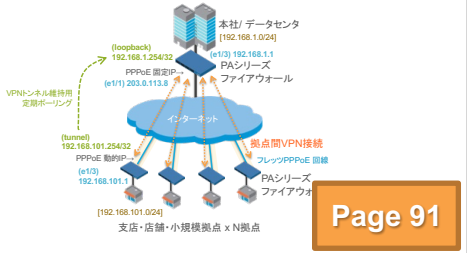
設定例 3



Page 55

公開サーバの保護2 (PPPoE Unnumbered 構成)

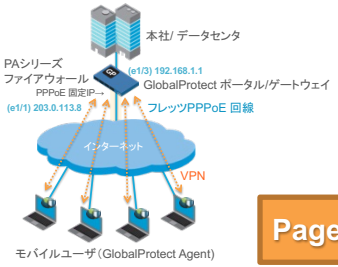
設定例 4



Page 91

拠点間 VPN 接続構成

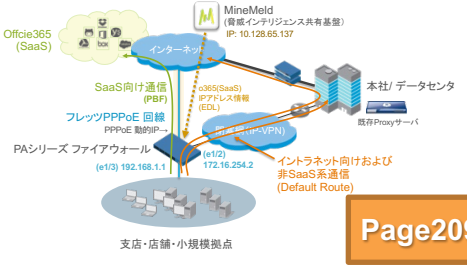
設定例 5



Page151

GlobalProtect によるモバイル環境の保護

設定例 6



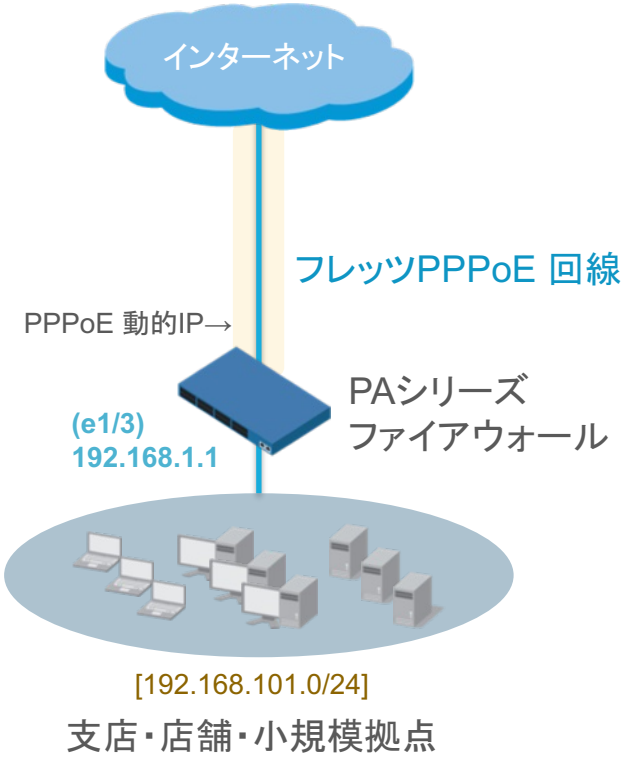
Page209

Office 365 ローカルブレイクアウト接続

PPPoE 設定例 1

中小規模拠点向けの
最もベーシックな接続構成

システム構成：



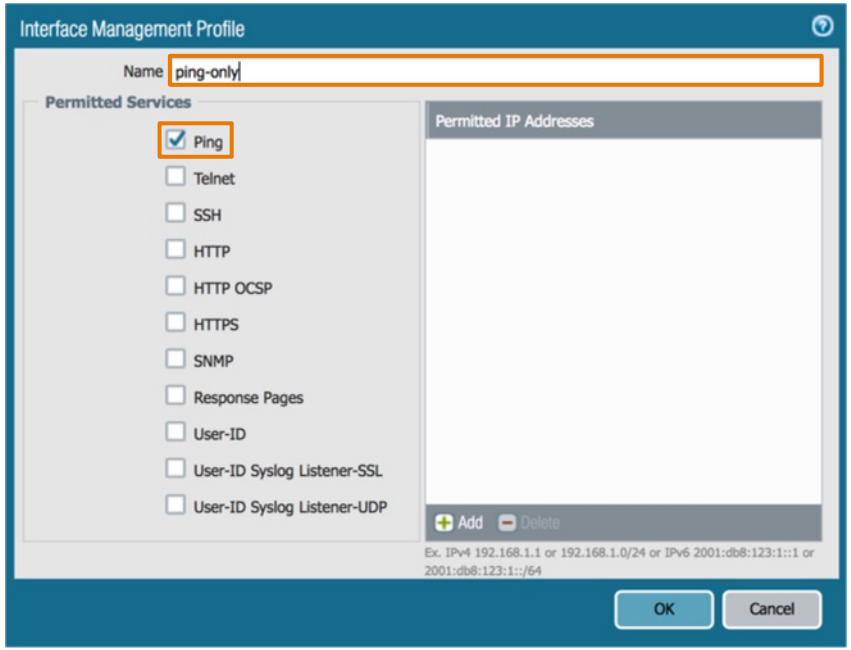
コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE関連	・MTU 値を必ず変更する（例：1454） ・PPPoE 認証方式はデフォルトのままで問題なし
その他	特になし

☆実環境においては、各種脅威防御やURLフィルタリング WildFireなど、重要なセキュリティ機能を必ず設定・ご利用下さい。

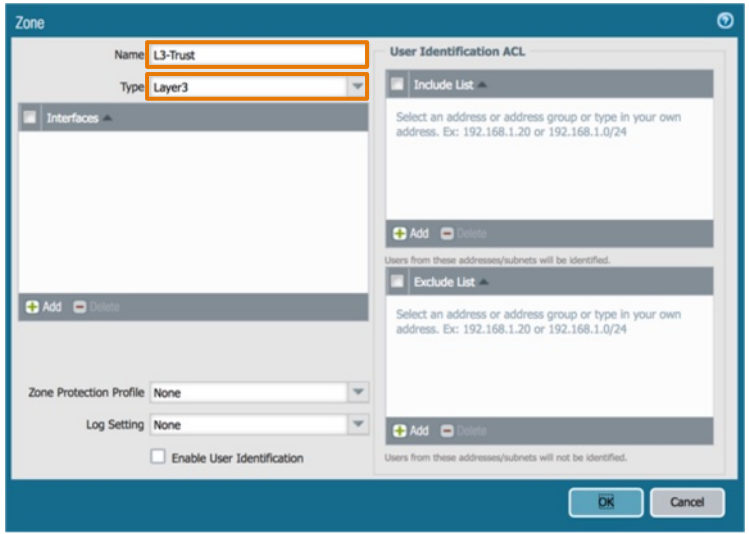
インターフェイス管理アクセス設定

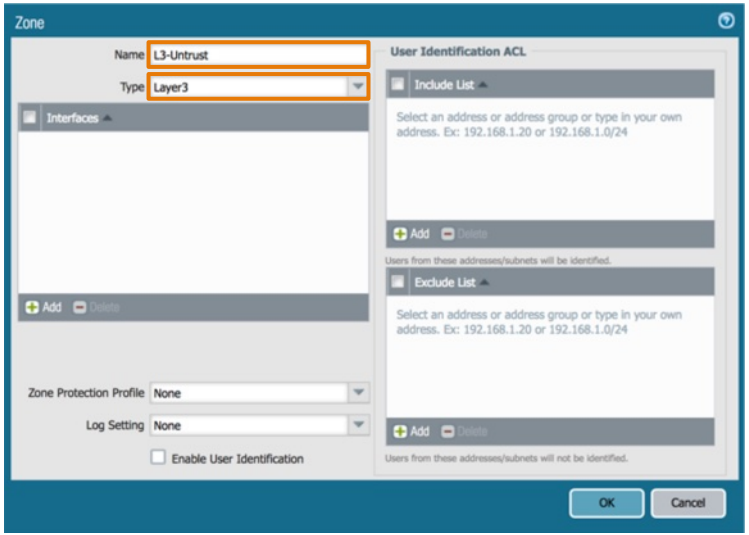
- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)



セキュリティゾーン設定

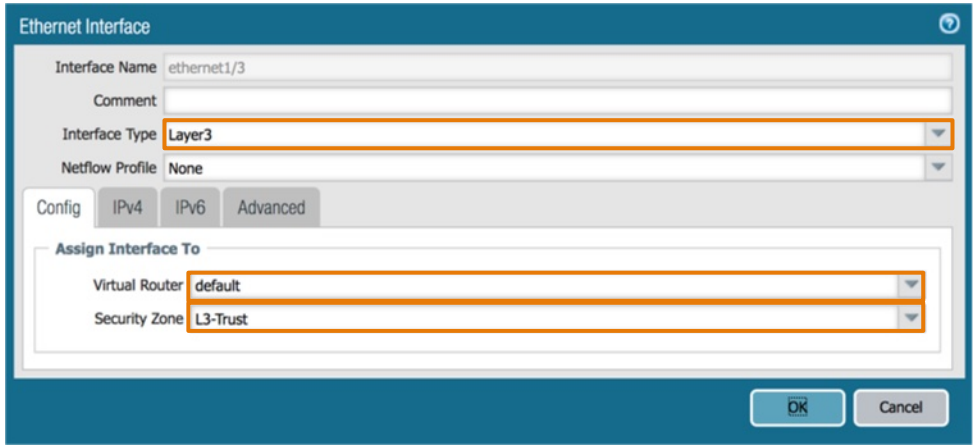
- 内部ネットワーク用、外部ネットワーク(インターネット)用セキュリティゾーンを作成 (Network > Zones)





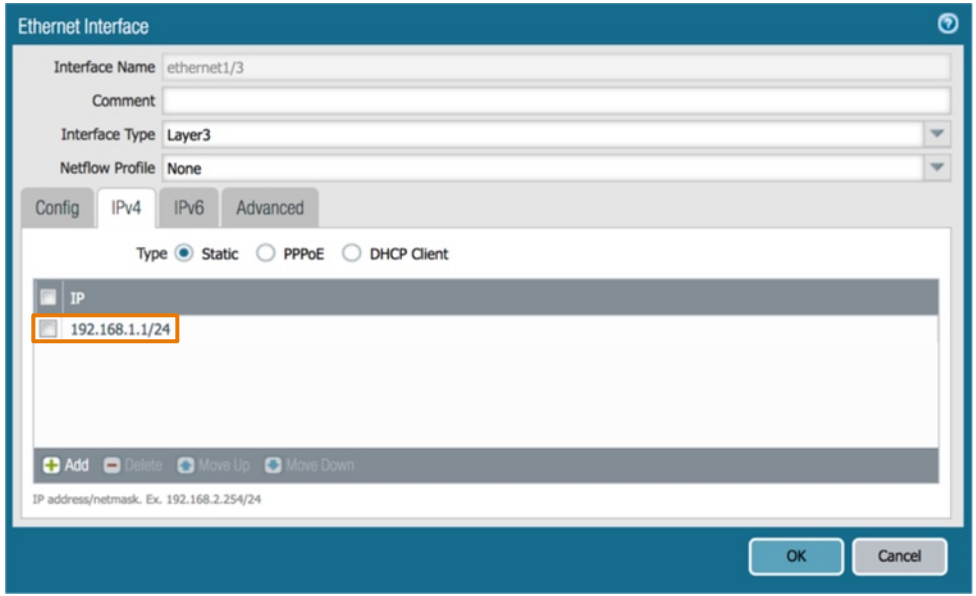
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



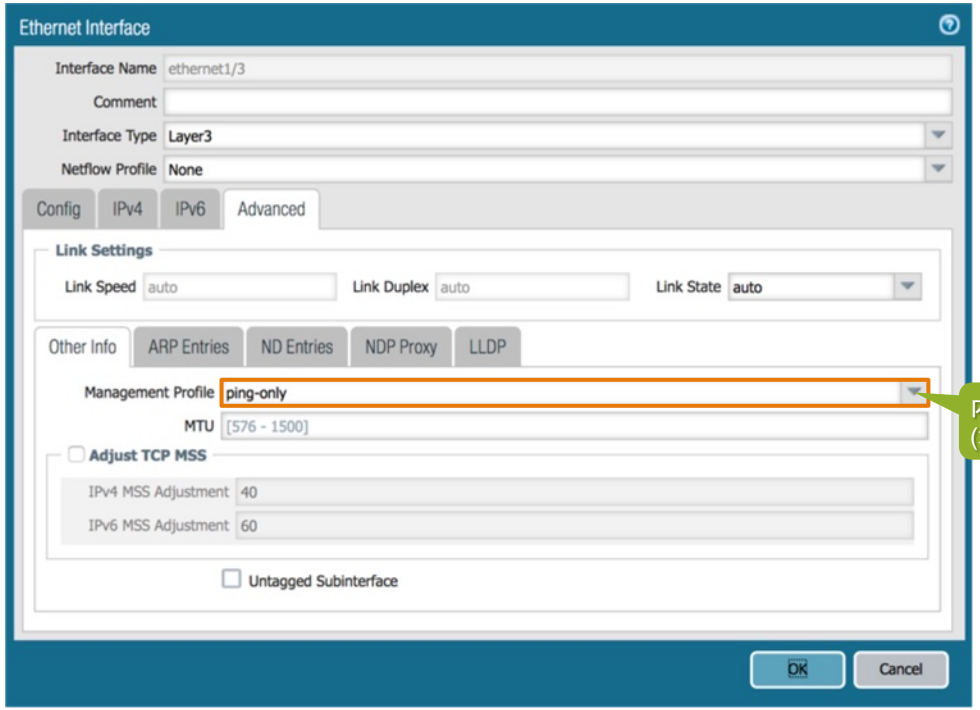
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



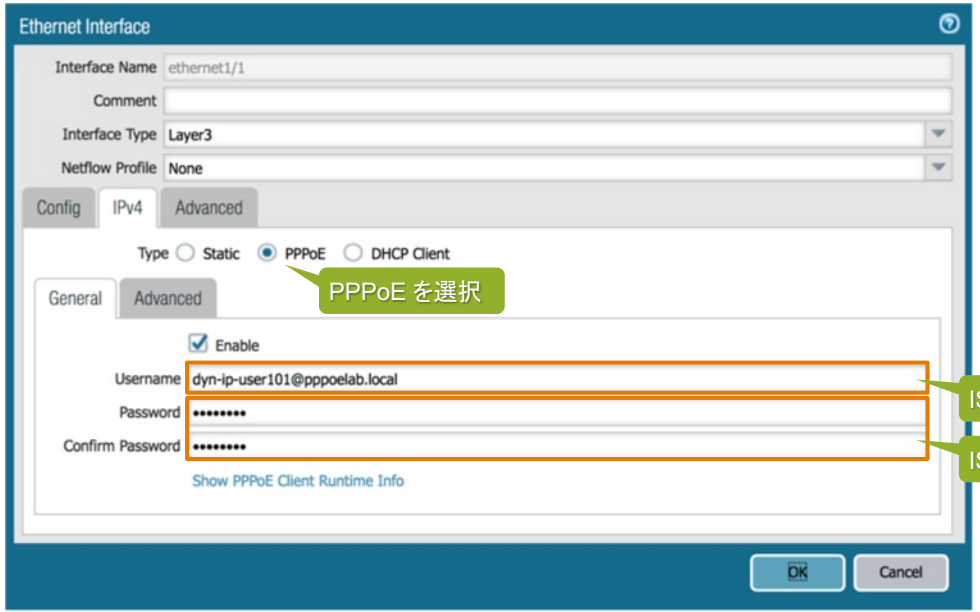
内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

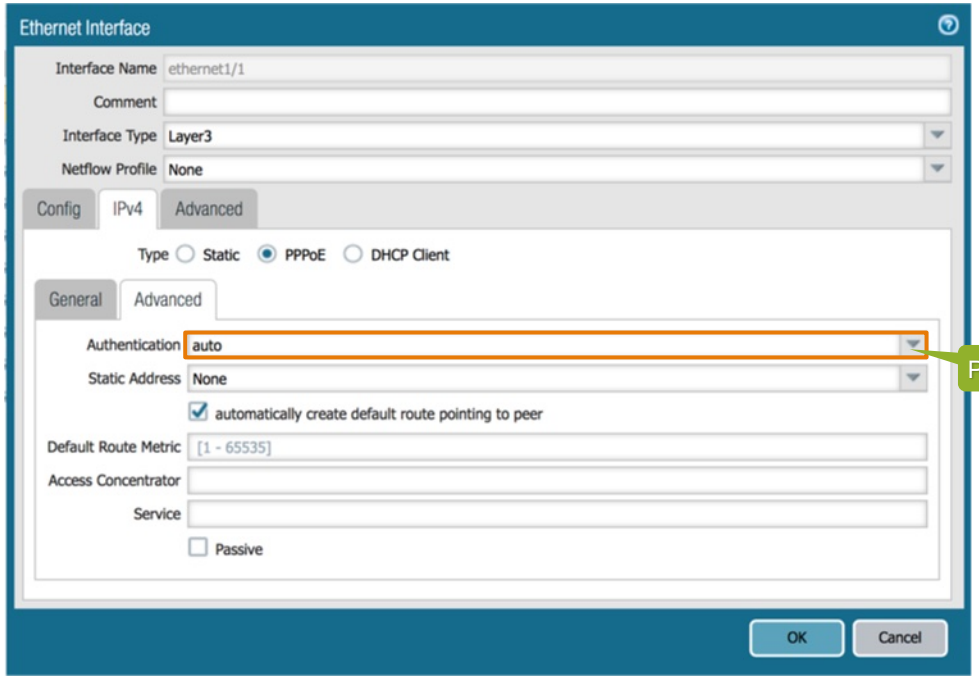


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

外部ネットワーク用インターフェイス設定

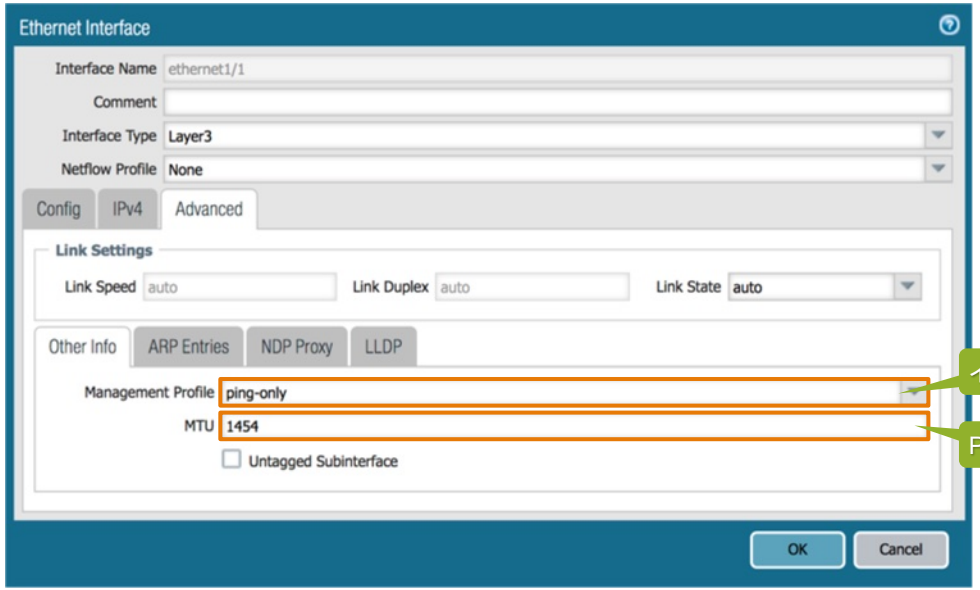
- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



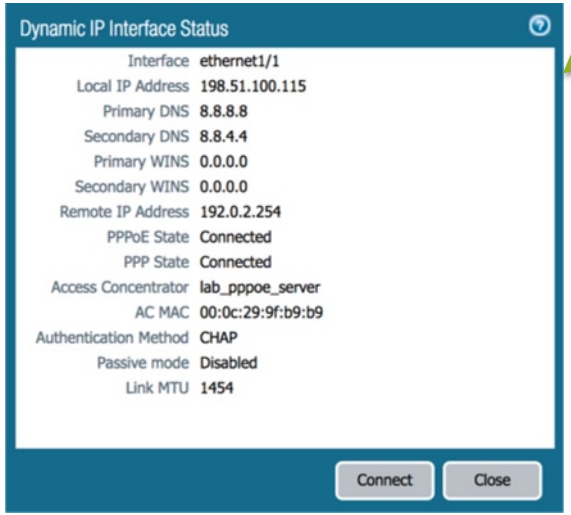
インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

ネットワークインターフェイス設定一覧

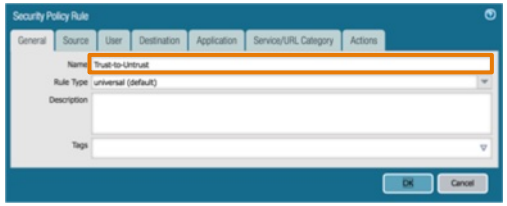
- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

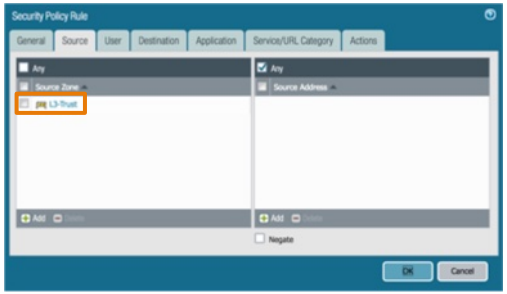
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone	Features
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	default	Untagged	L3-Untrust	
ethernet1/2				none	none	Untagged	none	
ethernet1/3	Layer3	ping-only		192.168.1.1/24	default	Untagged	L3-Trust	

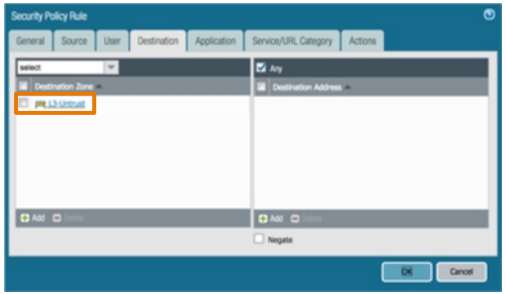


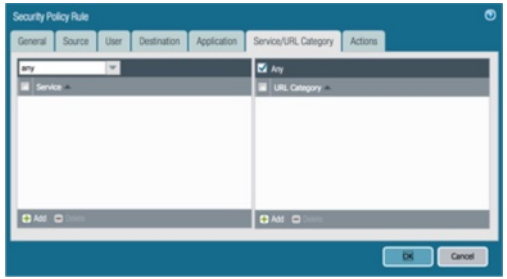
セキュリティポリシー設定

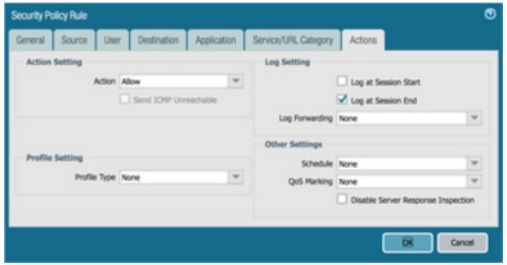
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)







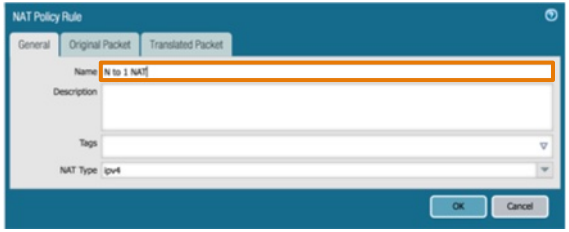


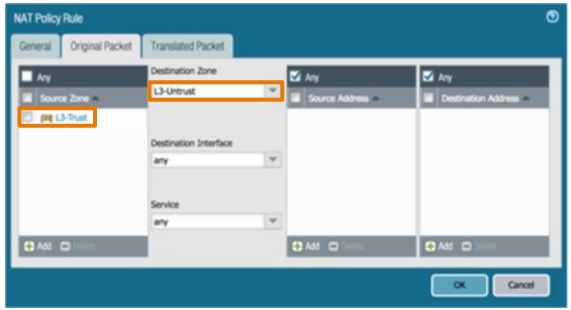


	Name	Tags	Type	Source			Destination		Application	Service	Action	Profile	Options
				Zone	Address	User	Zone	Address					
1	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
2	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
3	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)



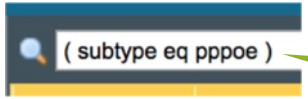


			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	none	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

設定後のPPPoE 接続ログ・接続状態

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/25 18:22:33	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:dyn-ip-user101@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:15, IP Address negotiated:198.51.100.115
03/25 18:22:29	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:dyn-ip-user101@pppoelab.local on interface:ethernet1/1

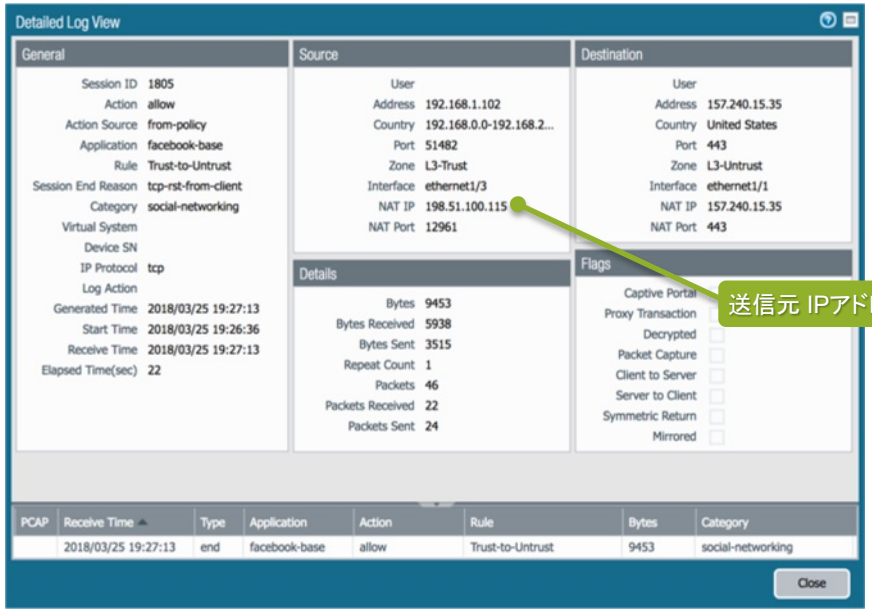


表示フィルタを使用することで必要なログを素早く確認することが可能

設定後のトラフィックログ例

- PPPoE 回線経由で通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/25 19:27:13	end	L3-Trust	L3-Untrust	192.168.1.102	157.240.15.35	443	facebook-base	social-networking	allow	Trust-to-Untrust	tcp-rst-from-client	9.5k

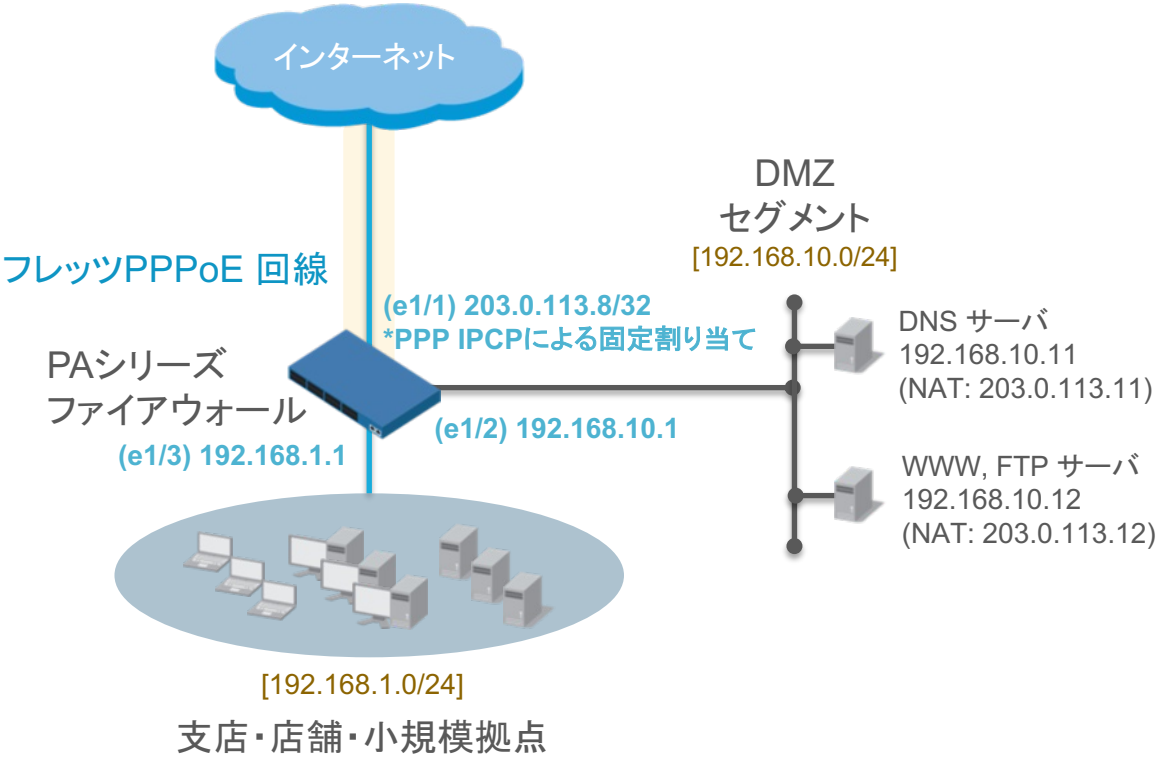


送信元 IPアドレスが PPPoE インターフェイスに割り当てられた IPアドレスに変換される

PPPoE 設定例２

セキュアなインターネット接続と
DMZセグメントによる公開サーバの保護

システム構成:



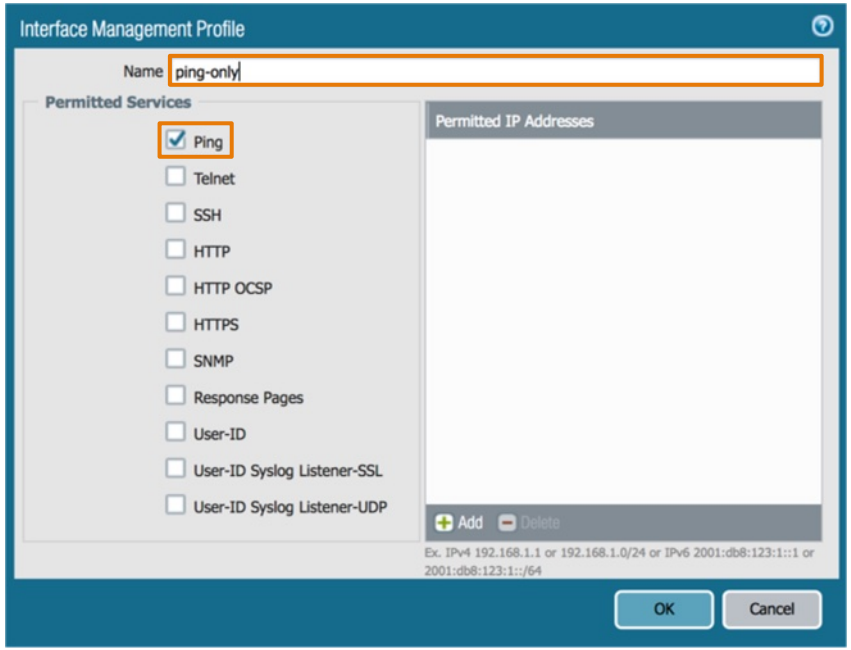
コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE関連	・MTU 値を必ず変更する（例：1454） ・PPPoE 認証方式はデフォルトのままで問題なし ・LAN型IPアドレス払い出し契約の場合先頭IPアドレス(ネットワークアドレス)がPPPoE インターフェイスにIPCPで割り当てられるが、PPPoEを有効にしているインターフェイスに明示的に設定する必要はない（設定しても問題はない）
その他	特になし

☆実環境においては、各種脅威防御やURLフィルタリング WildFireなど、重要なセキュリティ機能を必ず設定・ご利用下さい。

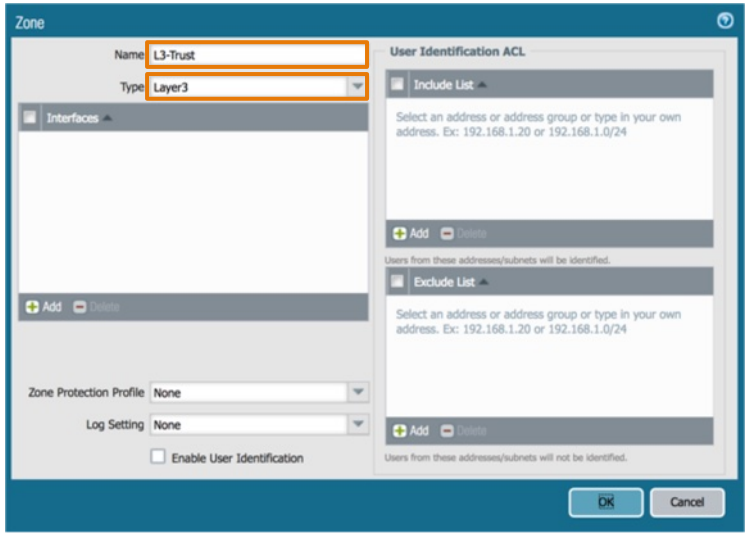
インターフェイス管理アクセス設定

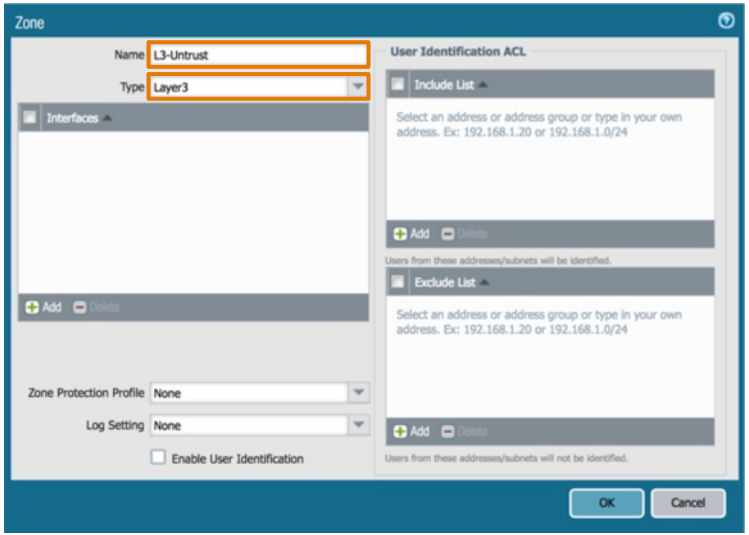
- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)



セキュリティゾーン設定

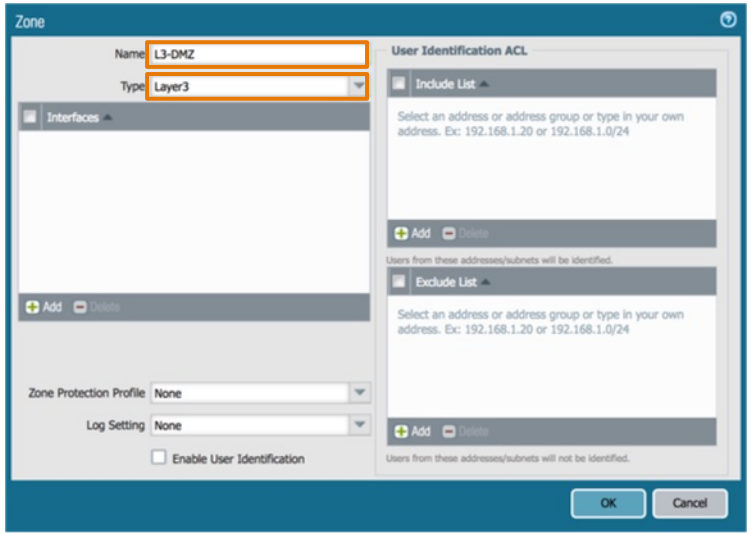
- 内部ネットワーク用、外部ネットワーク(インターネット)用セキュリティゾーンを作成 (Network > Zones)





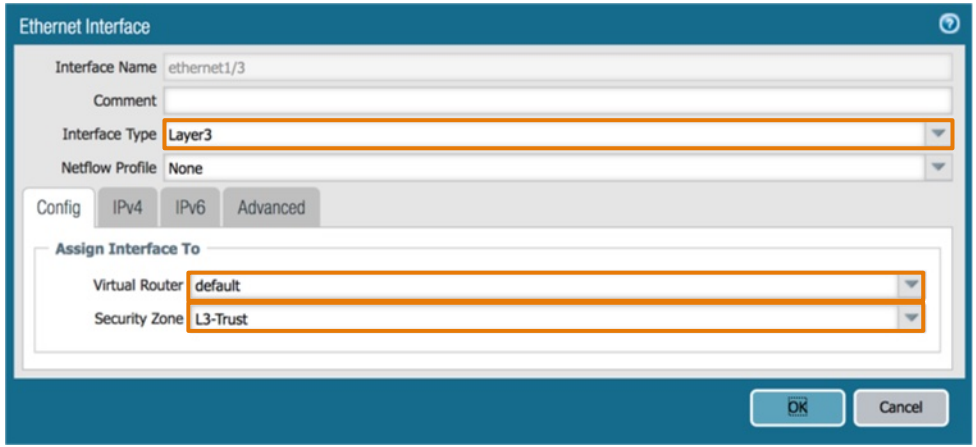
セキュリティゾーン設定

- 公開サーバ (DMZ) ネットワーク用セキュリティゾーンを作成 (Network > Zones)



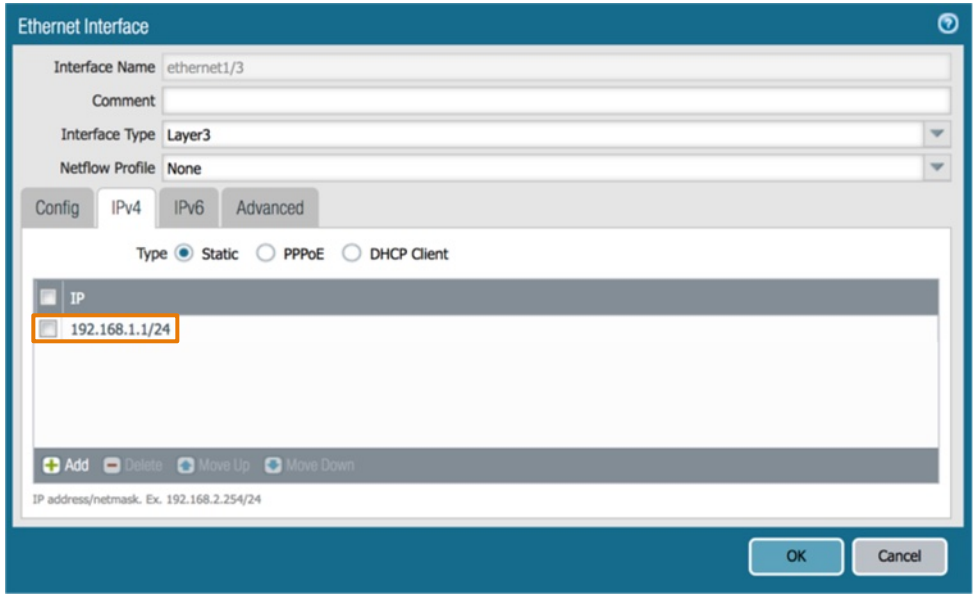
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



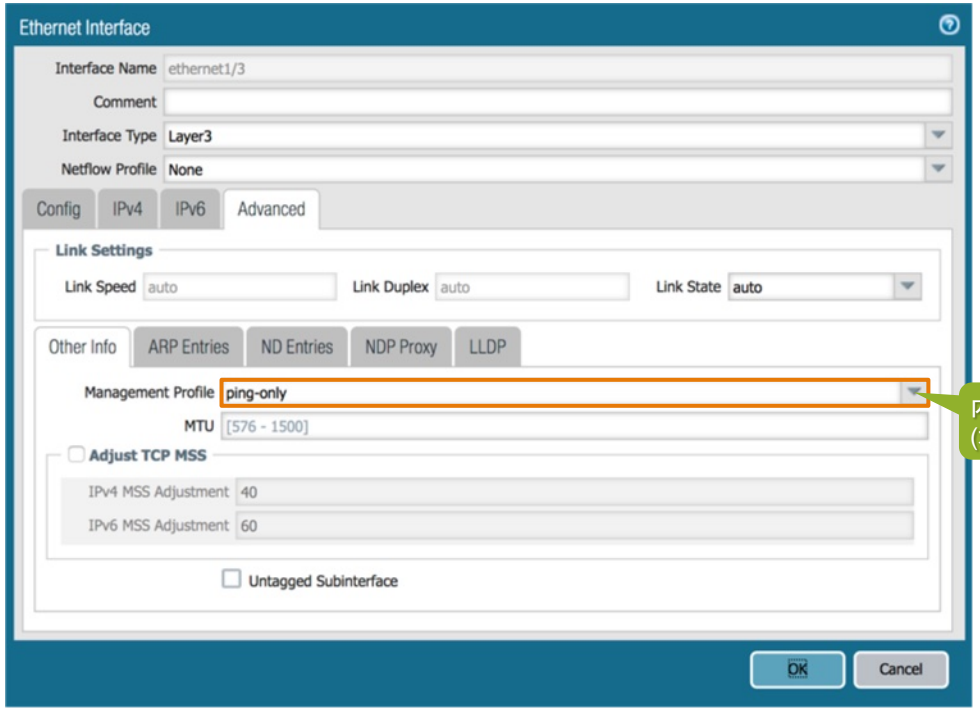
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク用インターフェイス設定

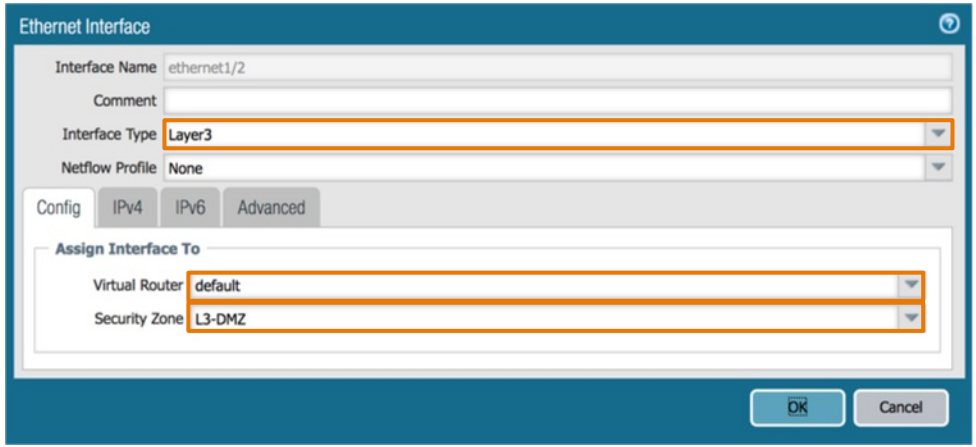
- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

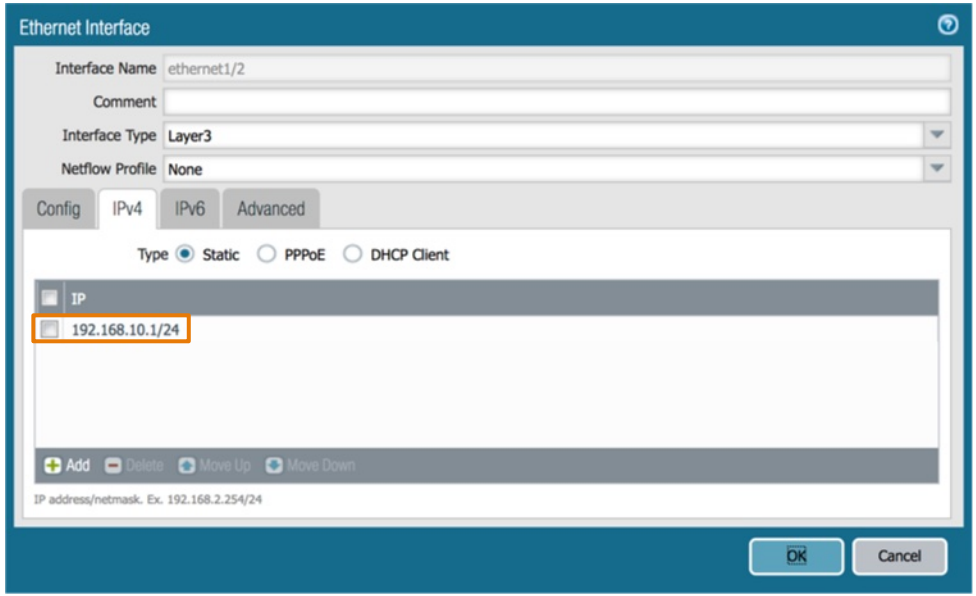
DMZネットワーク用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



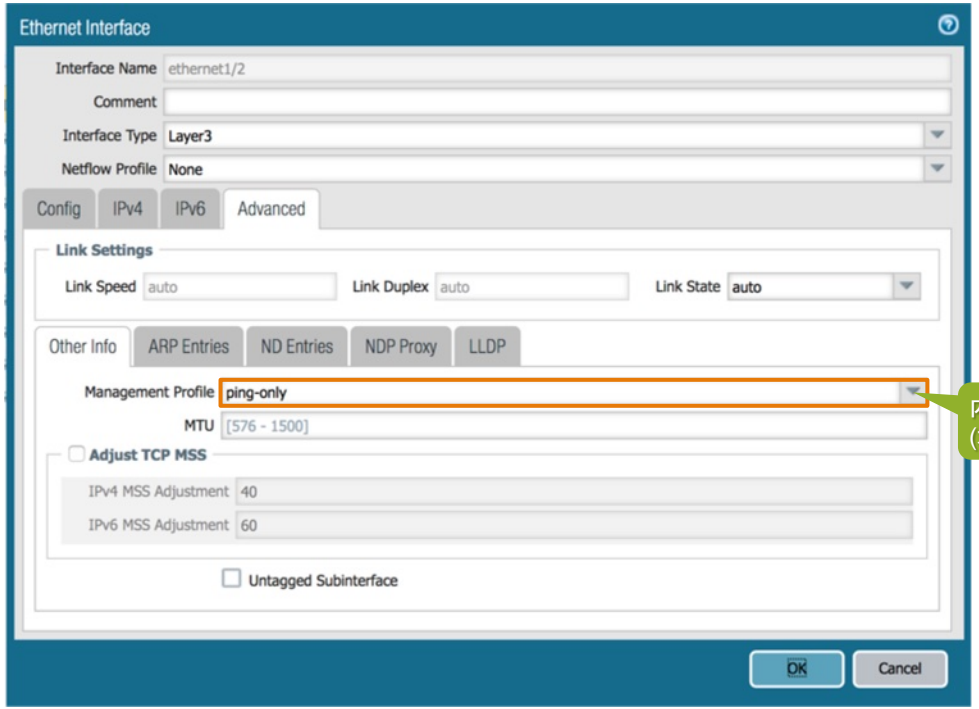
DMZネットワーク用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



DMZネットワーク用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



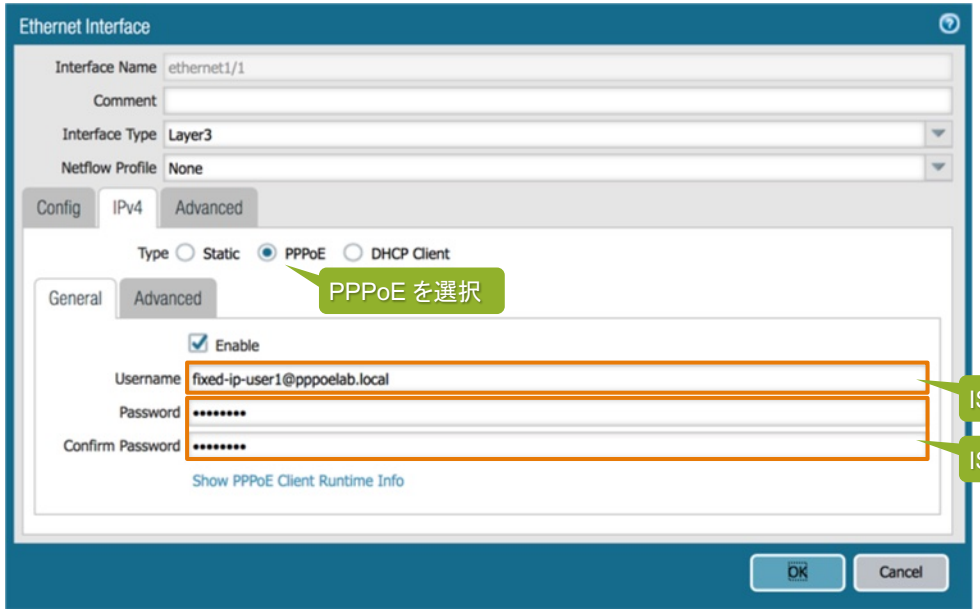
内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

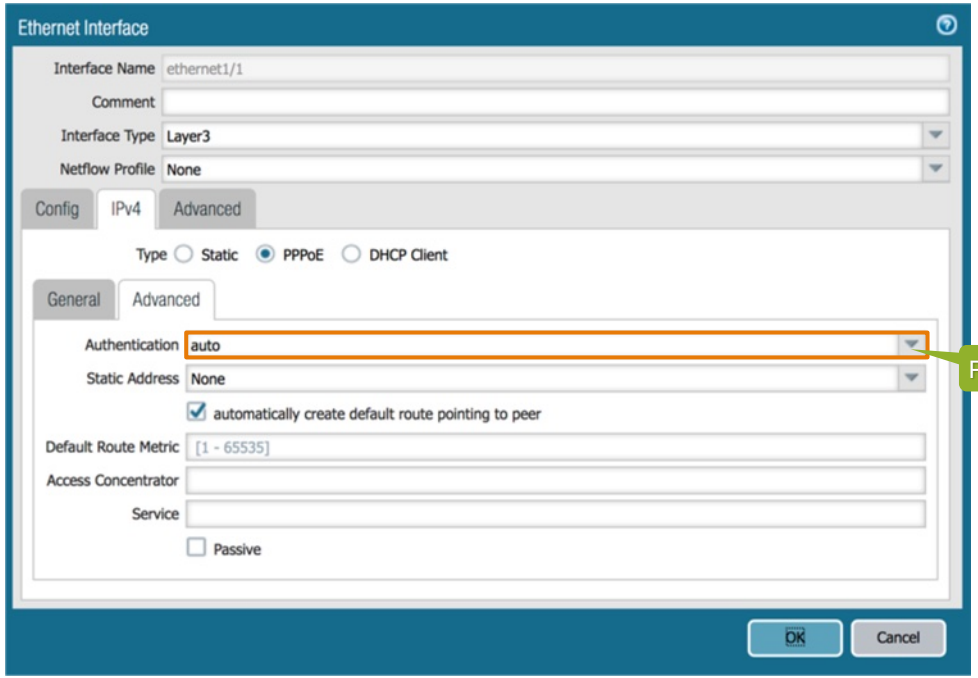


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

外部ネットワーク用インターフェイス設定

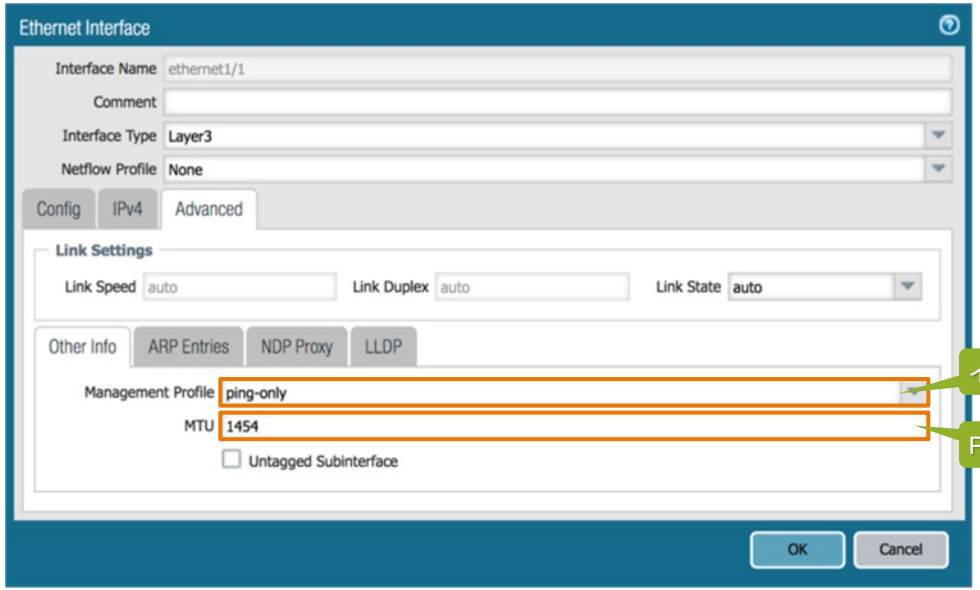
- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



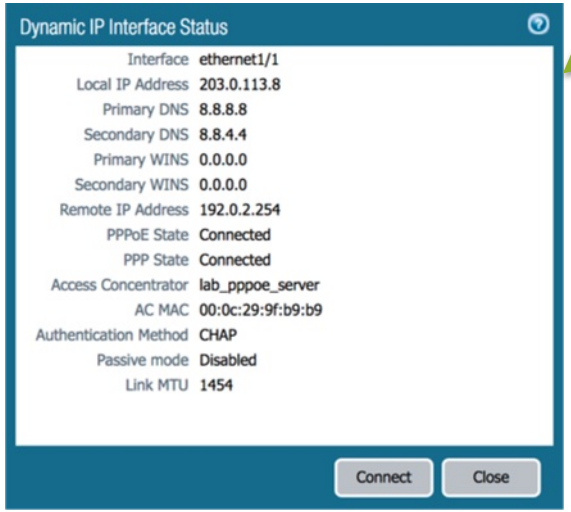
インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

ネットワークインターフェイス設定一覧

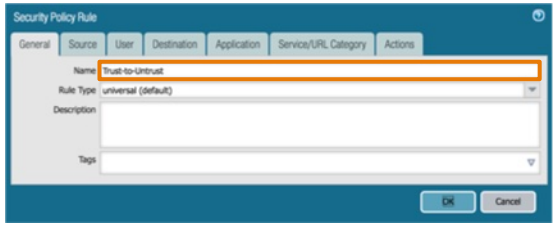
- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

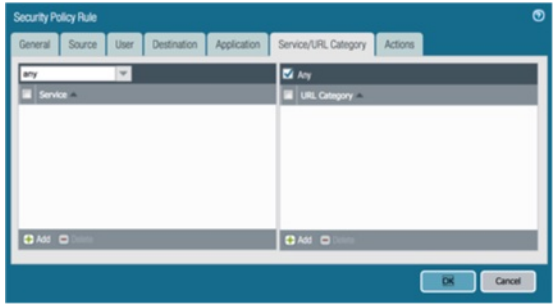
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone	Features
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	default	Untagged	L3-Untrust	
ethernet1/2	Layer3	ping-only		192.168.10.1/24	default	Untagged	L3-DMZ	
ethernet1/3	Layer3	ping-only		192.168.1.1/24	default	Untagged	L3-Trust	

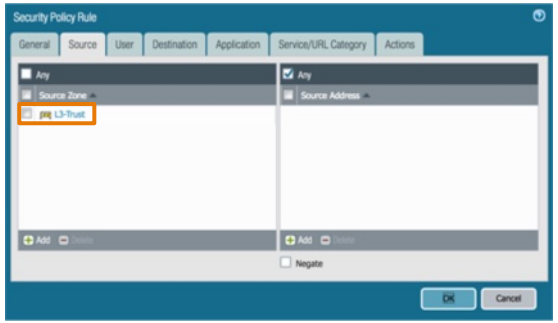


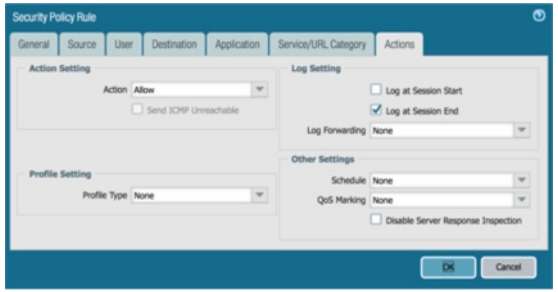
セキュリティポリシー設定

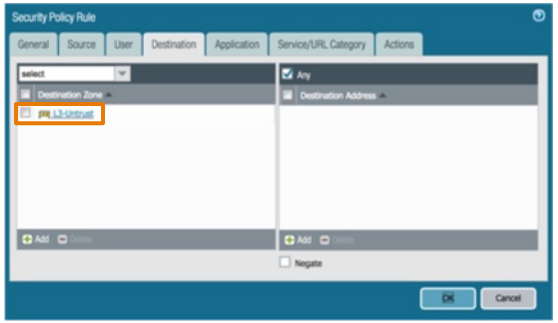
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)





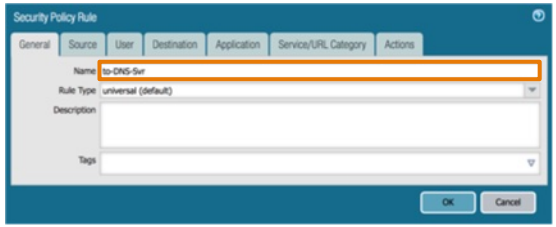


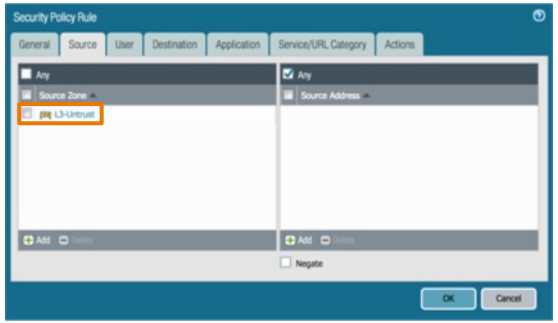


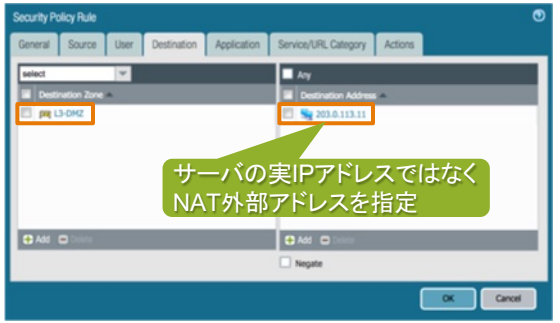


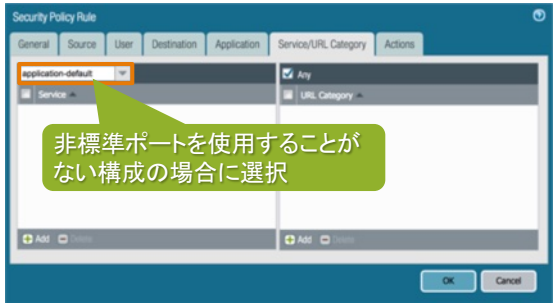
セキュリティポリシー設定

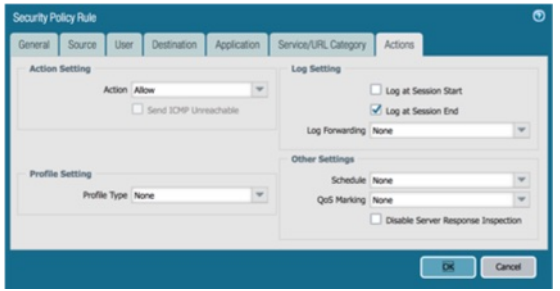
- 外部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)





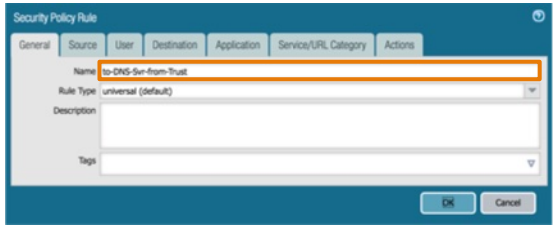


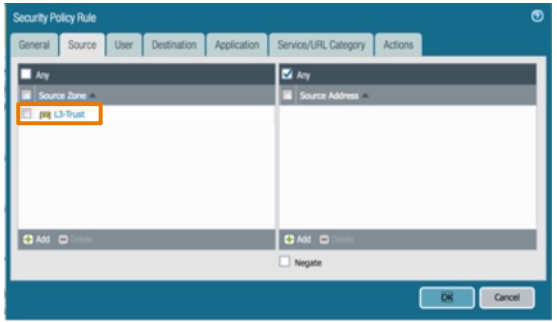


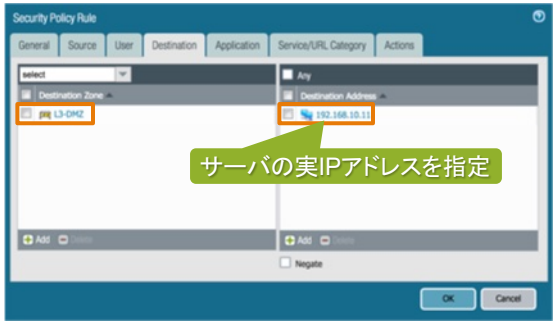


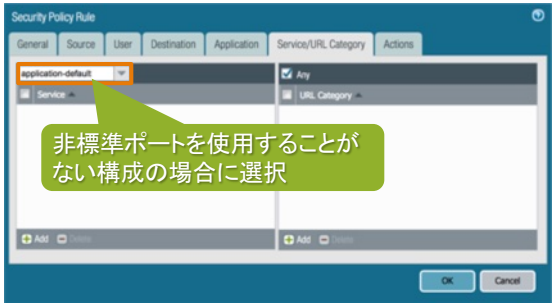
セキュリティポリシー設定

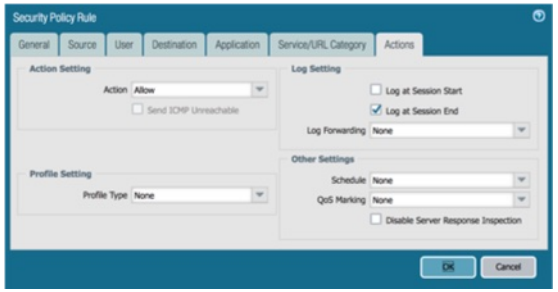
- 内部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)





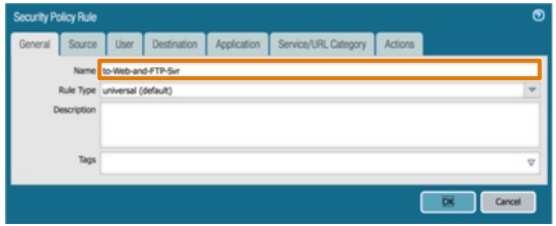


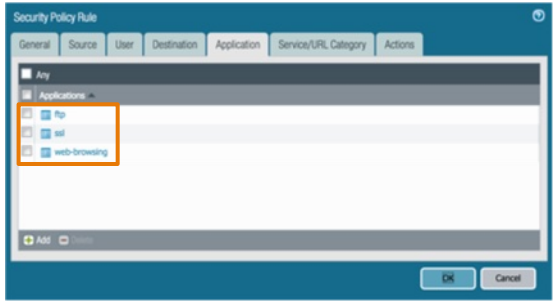


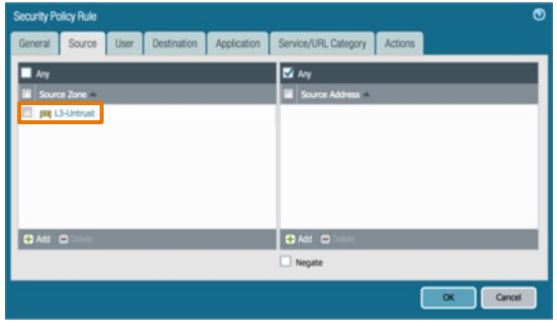


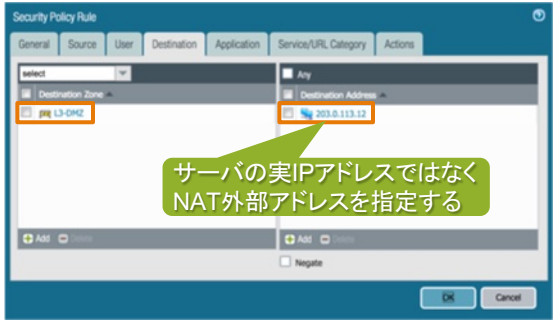
セキュリティポリシー設定

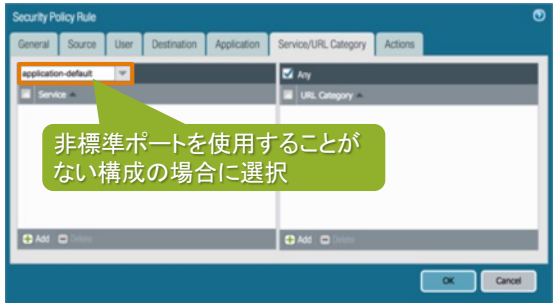
- 外部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)

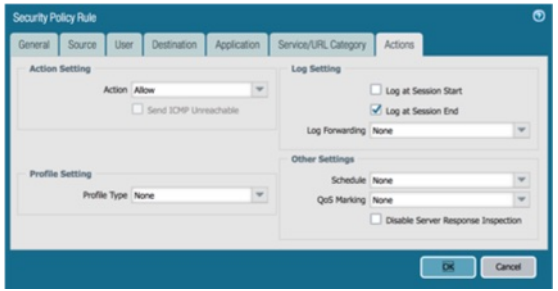






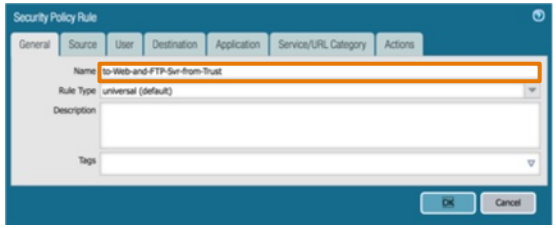


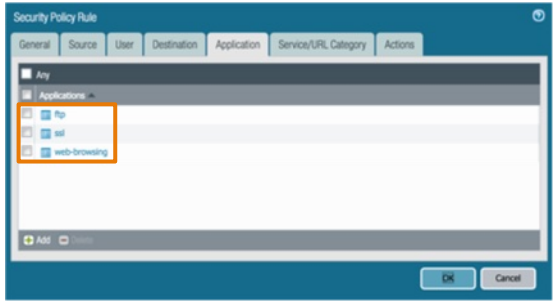


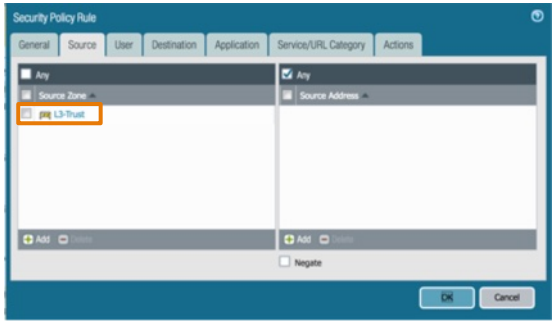


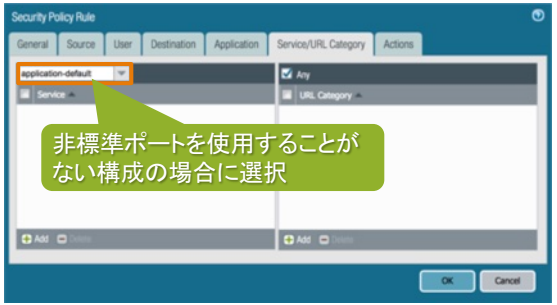
セキュリティポリシー設定

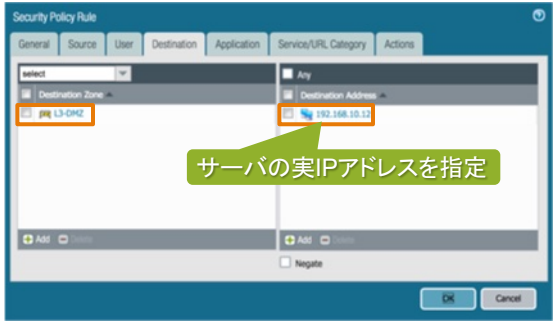
- 内部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)

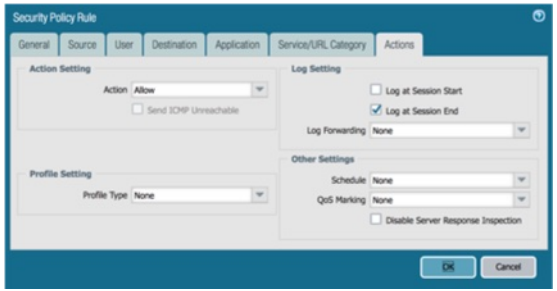






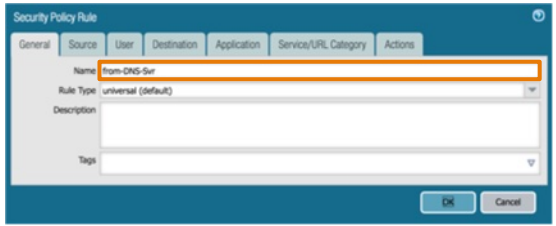


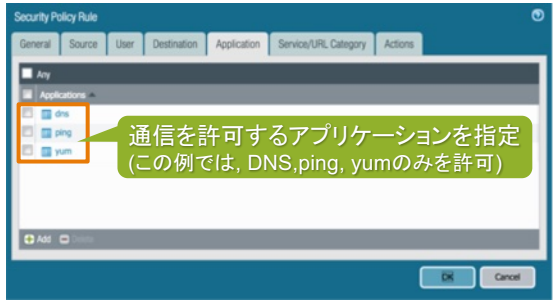


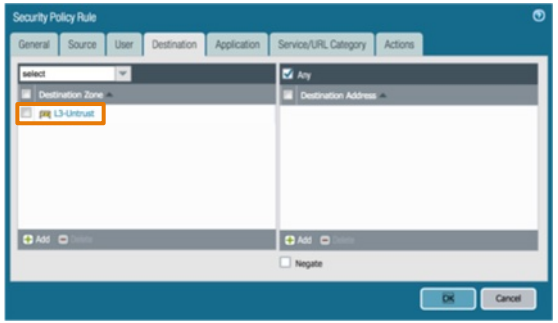


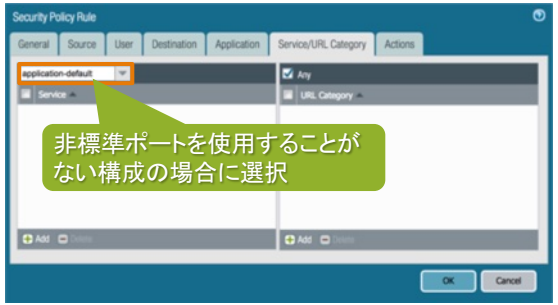
セキュリティポリシー設定

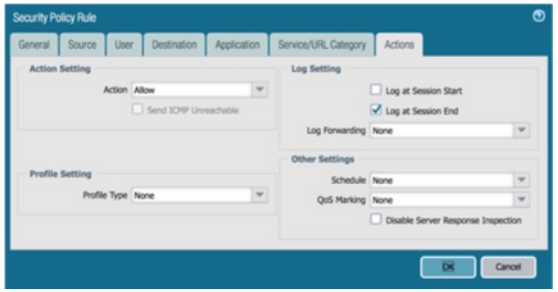
- DNSサーバ→外部向け通信用セキュリティポリシーの設定 (Policies > Security)





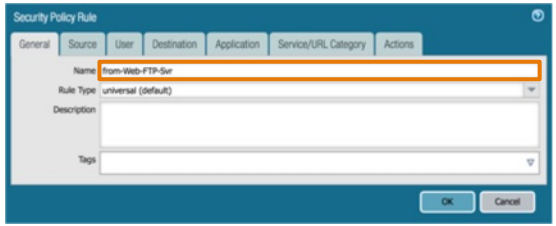


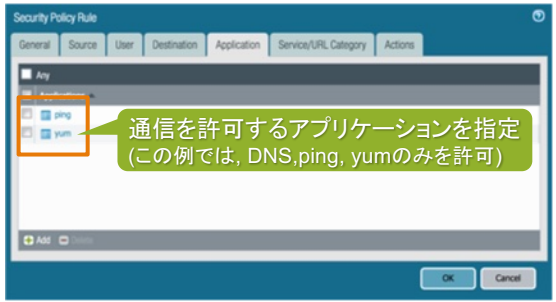


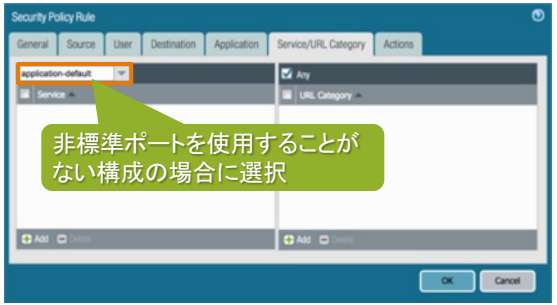


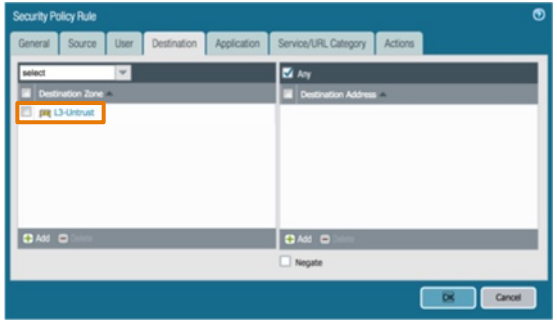
セキュリティポリシー設定

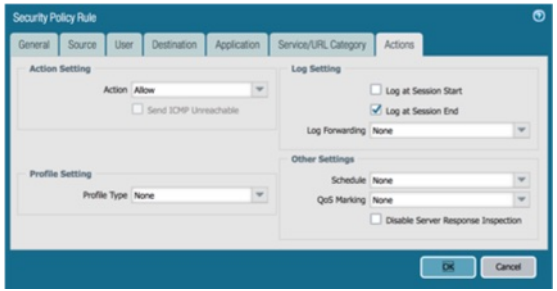
- Web/FTPサーバ→外部向け通信用セキュリティポリシーの設定 (Policies > Security)











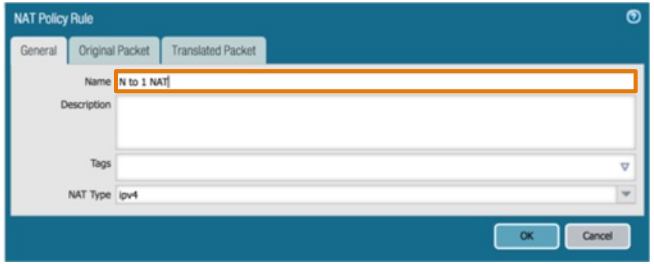
セキュリティポリシー設定一覧

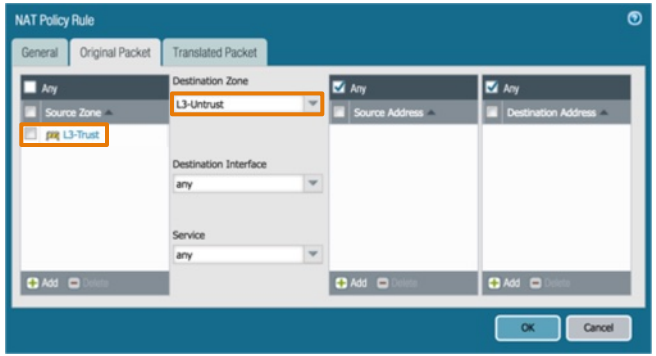
- セキュリティポリシー設定一覧 (Policies > Security)

				Source			Destination						
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
2	to-DNS-Svr	none	universal	L3-Untrust	any	any	L3-DMZ	203.0.113.11	dns	application-default	Allow	none	
3	to-DNS-Svr-from-Trust	none	universal	L3-Trust	any	any	L3-DMZ	192.168.10.11	dns	application-default	Allow	none	
4	to-Web-and-FTP-Svr	none	universal	L3-Untrust	any	any	L3-DMZ	203.0.113.12	ftp ssl web-browsing	application-default	Allow	none	
5	to-Web-and-FTP-Svr-from-Trust	none	universal	L3-Trust	any	any	L3-DMZ	192.168.10.12	ftp ssl web-browsing	application-default	Allow	none	
6	from-DNS-Svr	none	universal	L3-DMZ	192.168.10.11	any	L3-Untrust	any	dns ping yum	application-default	Allow	none	
7	from-Web-FTP-Svr	none	universal	L3-DMZ	192.168.10.12	any	L3-Untrust	any	ping yum	application-default	Allow	none	
8	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
9	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)

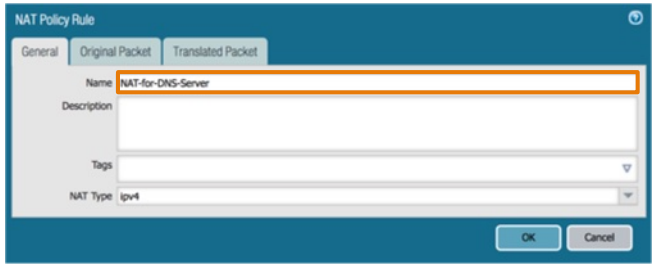


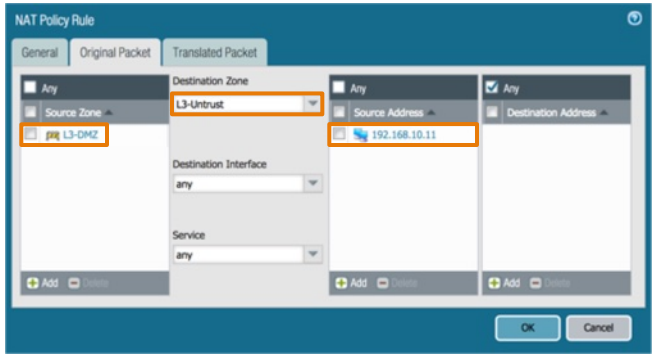


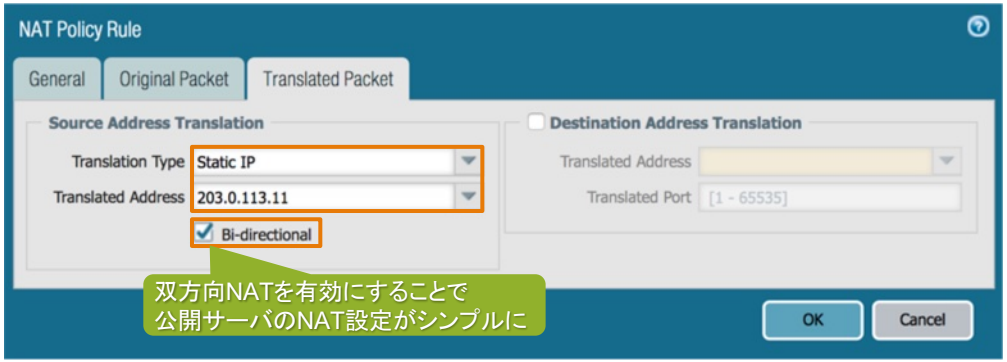
IPアドレスは指定しなくて良い
(インターフェイス に割当てられた
IPアドレスが自動的に使われる)

NATポリシー設定

- DMZセグメント DNSサーバ用 NATポリシーの設定 (Policies > NAT)

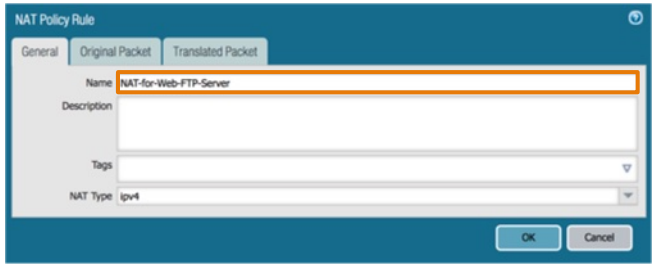


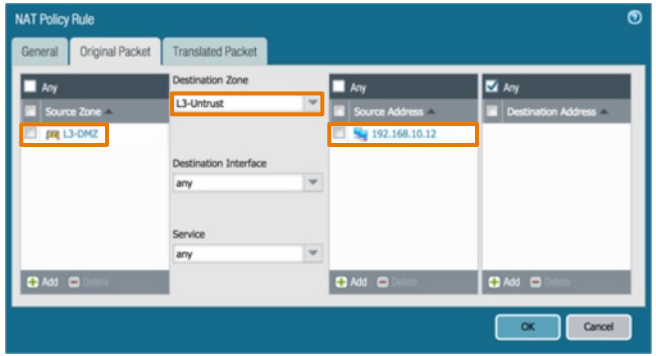


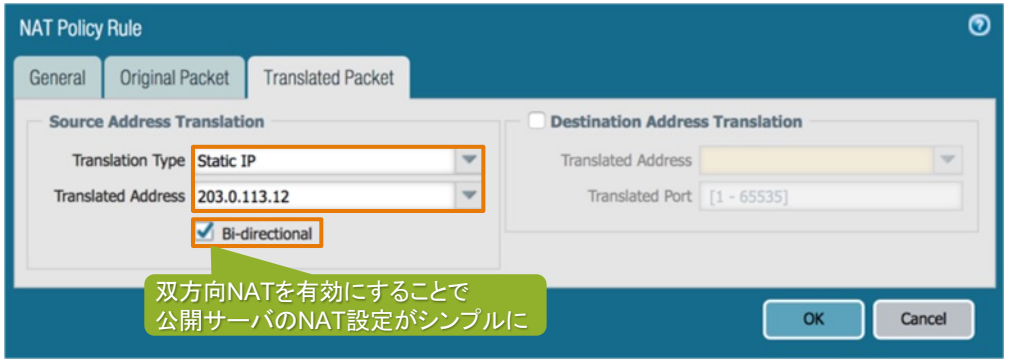


NATポリシー設定

- DMZセグメント Web/FTPサーバ用 NATポリシーの設定 (Policies > NAT)







NATポリシー設定一覧

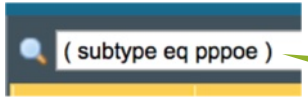
- NATポリシー設定一覧 (Policies > NAT)

		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none
2	NAT-for-DNS-Server	L3-DMZ	L3-Untrust	any	192.168.10.11	any	any	static-ip 203.0.113.11 bi-directional: yes	none
3	NAT-for-Web-FTP-Server	L3-DMZ	L3-Untrust	any	192.168.10.12	any	any	static-ip 203.0.113.12 bi-directional: yes	none

設定後のPPPoE 接続ログ・接続状態

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/25 21:05:59	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:16, IP Address negotiated:203.0.113.8
03/25 21:05:55	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1

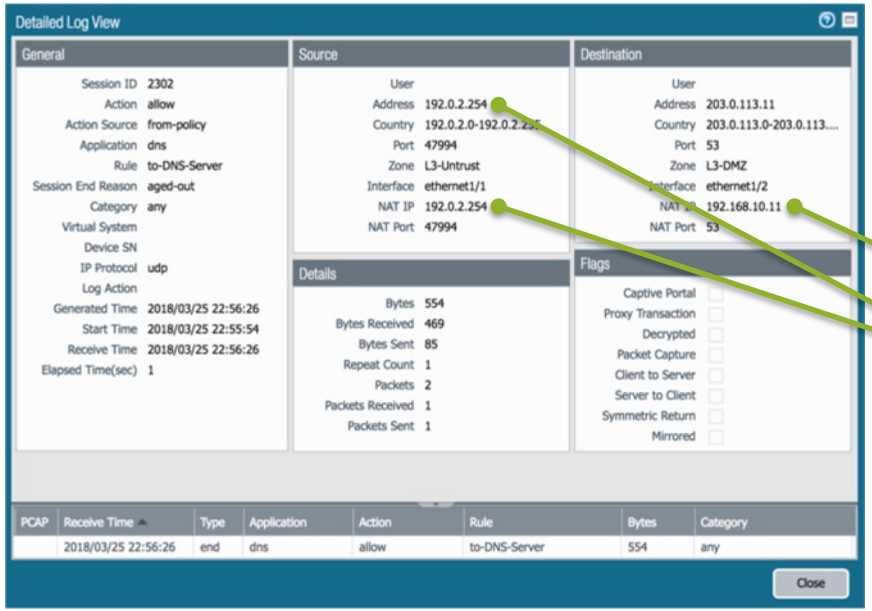


表示フィルタを使用することで必要なログを素早く確認することが可能

設定後のトラフィックログ例

- 外部からDMZ上のDNSサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/25 22:56:26	end	L3-Untrust	L3-DMZ	192.0.2.254	203.0.113.11	53	dns	any	allow	to-DNS-Server	aged-out	554



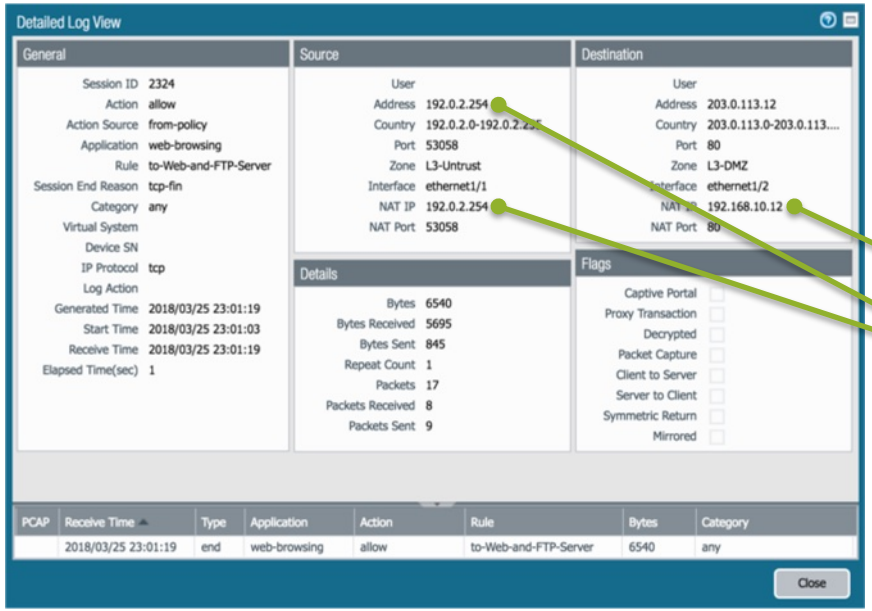
宛先 IPアドレスがサーバ実 IPアドレスに変換される

送信元 IPアドレスはオリジナルのまま

設定後のトラフィックログ例

- 外部からDMZ上のWeb/FTPサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/25 23:01:19	end	L3-Untrust	L3-DMZ	192.0.2.254	203.0.113.12	80	web-browsing	any	allow	to-Web-and-FTP-Server	tcp-fin	6.5k



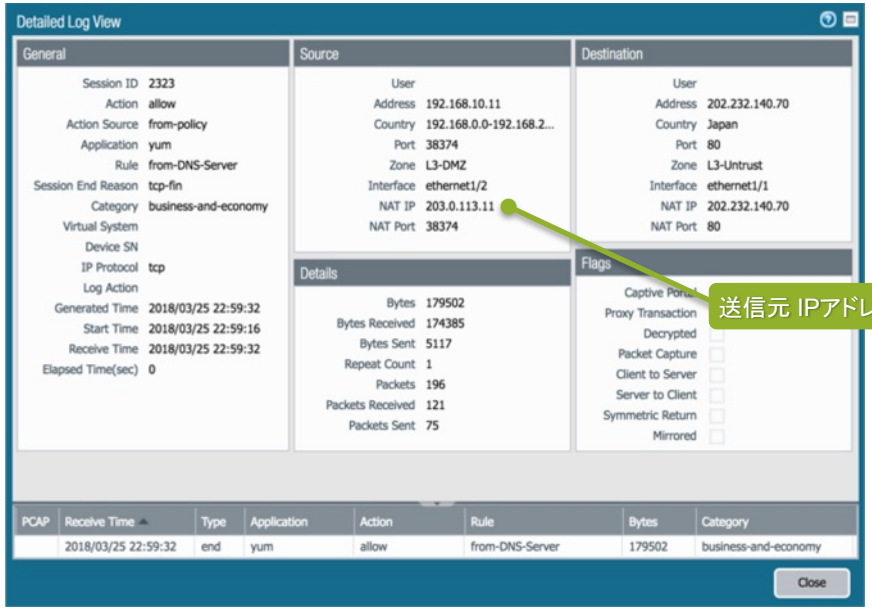
宛先 IPアドレスがサーバ実 IPアドレスに変換される

送信元 IPアドレスはオリジナルのまま

設定後のトラフィックログ例

- DMZ上のDNSサーバから外部側へ通信した場合のログ例 (Monitor > Logs > Traffic)

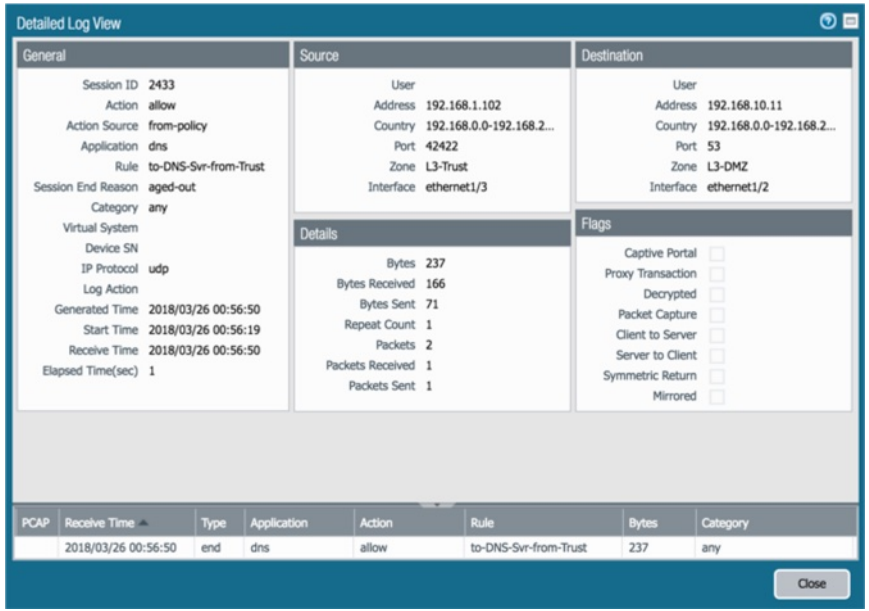
		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/25 22:59:32	end	L3-DMZ	L3-Untrust	192.168.10.11	202.232.140.70	80	yum	business-and-economy	allow	from-DNS-Server	tcp-fin	179.5k



設定後のトラフィックログ例

- 内部からDMZ上のDNSサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

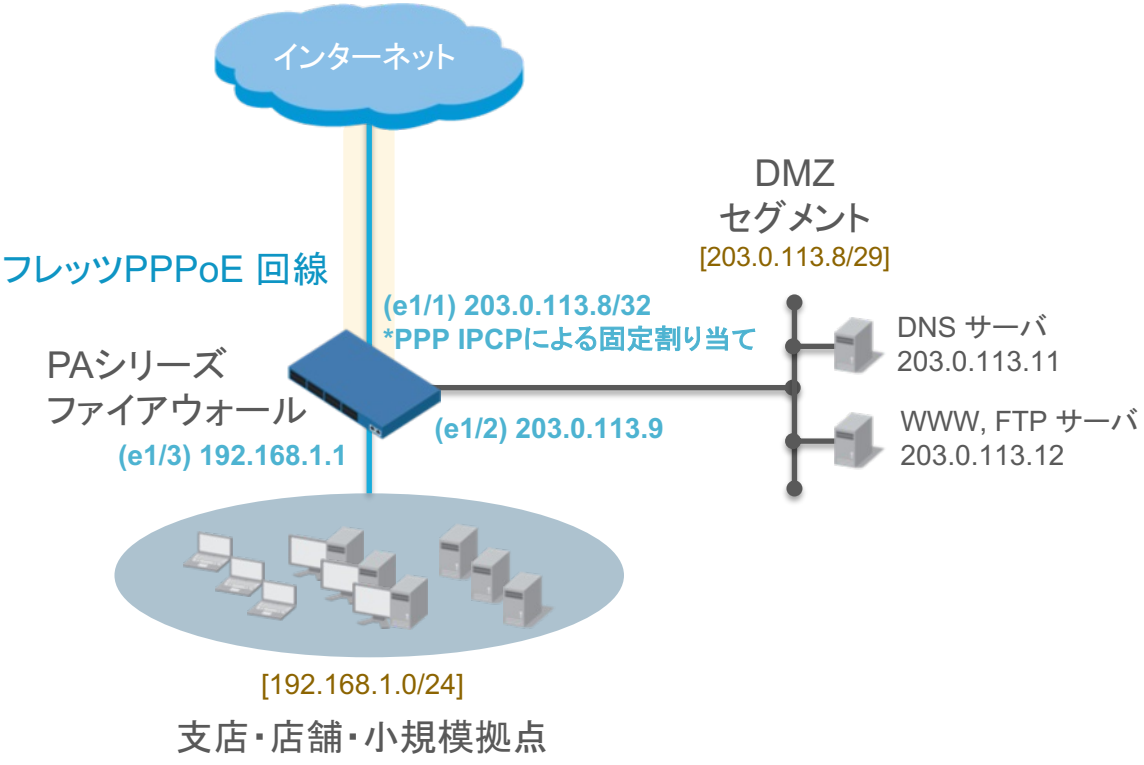
		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 00:56:50	end	L3-Trust	L3-DMZ	192.168.1.102	192.168.10.11	53	dns	any	allow	to-DNS-Svr-from-Trust	aged-out	237



PPPoE 設定例３

セキュアなインターネット接続と
Global IPアドレスを定義した公開サーバの保護
(PPPoE Unnumbered 接続)

システム構成：



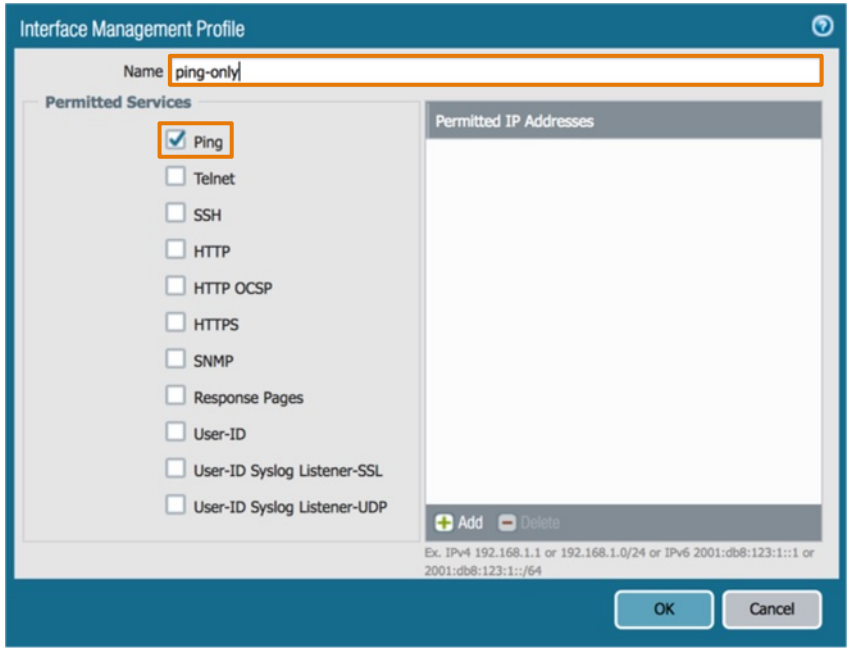
コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE 関連	・MTU 値を必ず変更する（例：1454） ・PPPoE 認証方式はデフォルトのままで問題なし ・LAN型IPアドレス払い出し契約の場合先頭IPアドレス(ネットワークアドレス)がPPPoE インターフェイスにIPCPで割り当てられるが、PPPoEを有効にしているインターフェイスに明示的に設定する必要はない（設定しても問題はない）
その他	・必ず2つの仮想ルータを定義し、仮想ルータ間のStatic Routing を設定する ・内部ネットワーク→インターネット向け通信のNAT外部アドレスとしてPPPoE インターフェイスに割り当てられたIPアドレスのほか、ISPから割り当てられ他のGlobal IP (例: PAのDMZ I/F IPアドレス)を使用することも可能

☆実環境においては、各種脅威防御やURLフィルタリング WildFireなど、重要なセキュリティ機能を必ず設定・ご利用下さい。

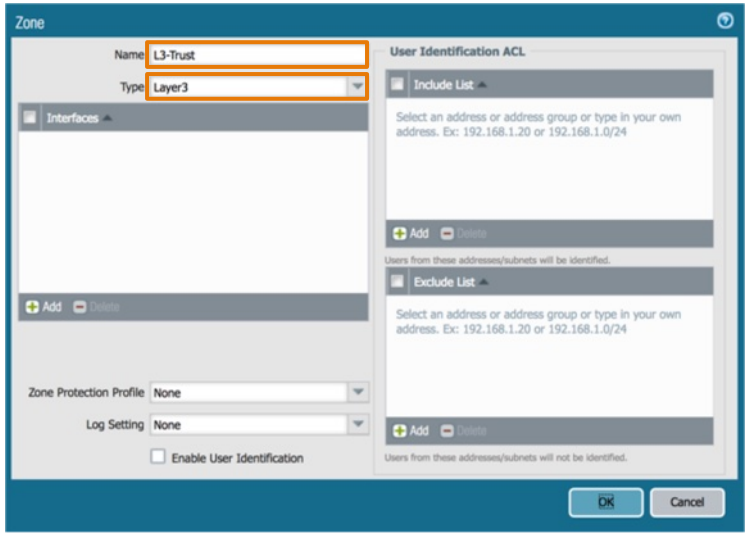
インターフェイス管理アクセス設定

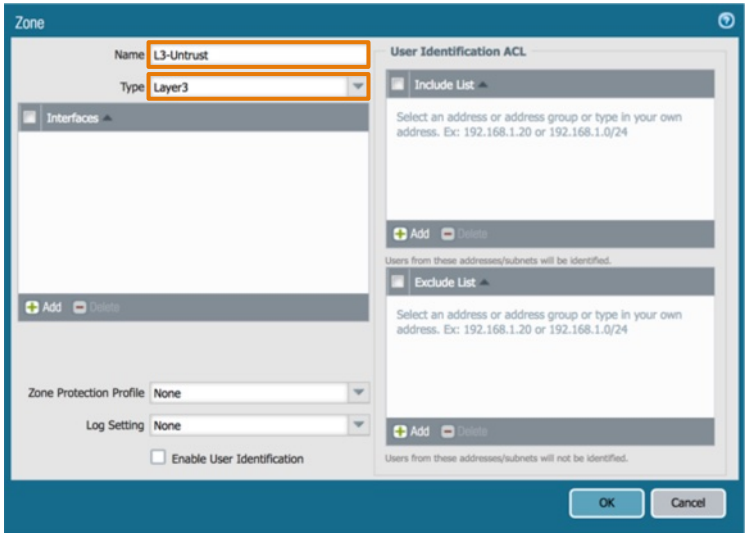
- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)



セキュリティゾーン設定

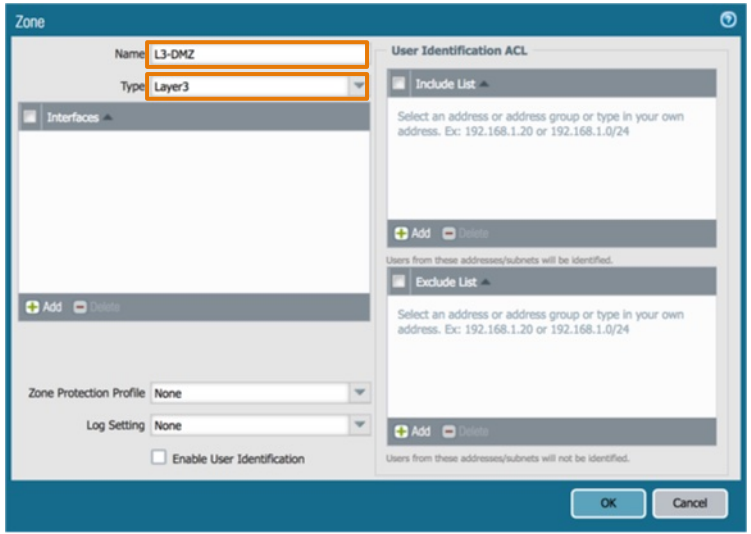
- 内部ネットワーク用、外部ネットワーク(インターネット)用セキュリティゾーンを作成 (Network > Zones)





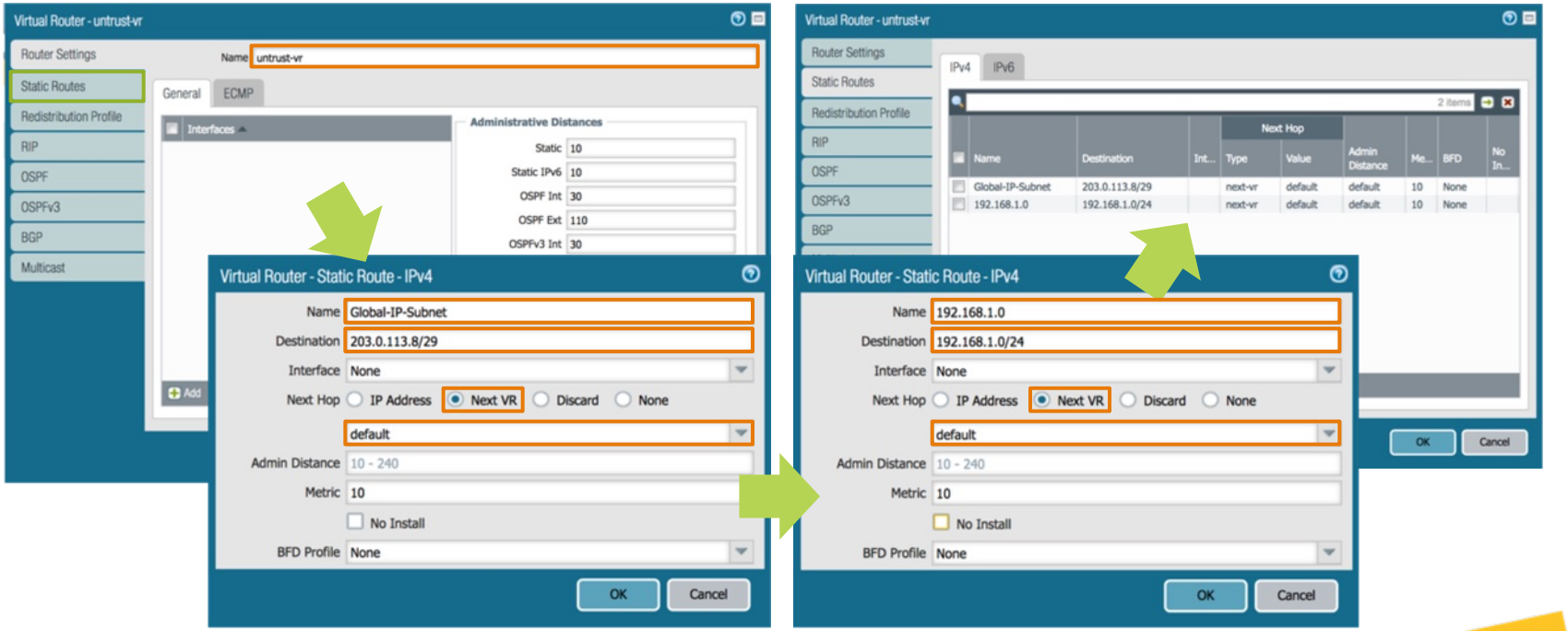
セキュリティゾーン設定

- 公開サーバ (DMZ) ネットワーク用セキュリティゾーンを作成 (Network > Zones)



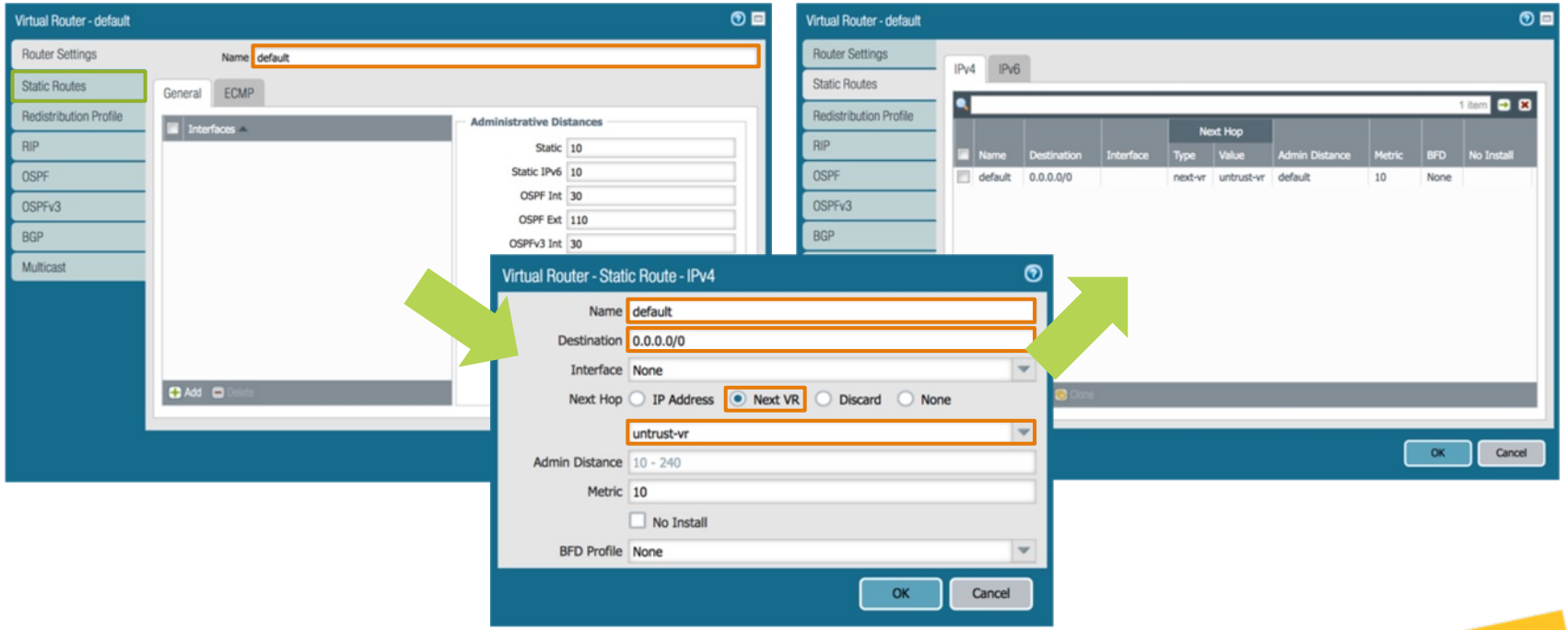
仮想ルーター設定

- PPPoE 回線接続用仮想ルーター ”untrust-vr” を作成し、DMZ向けおよび内部IPサブネット向けStatic Routeを追加 (Network > Virtual Routers)



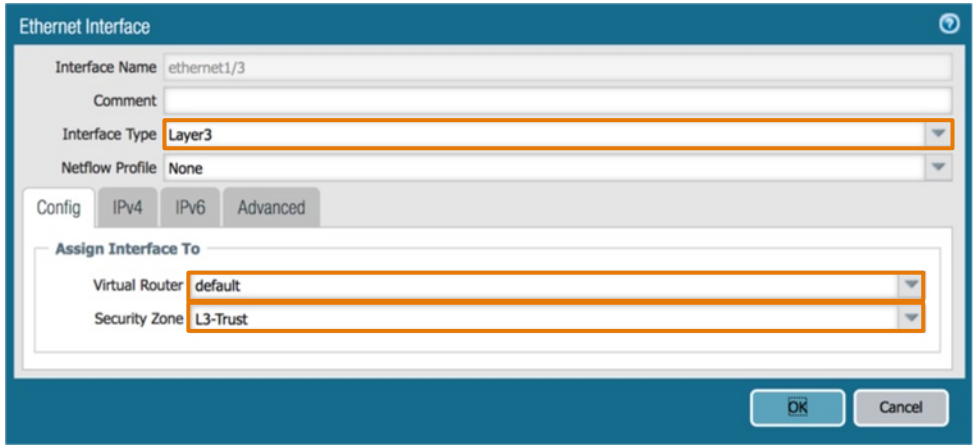
仮想ルーター設定

- デフォルト仮想ルーター ”default” に対してインターネット向けStatic Routeを追加 (Network > Virtual Routers)



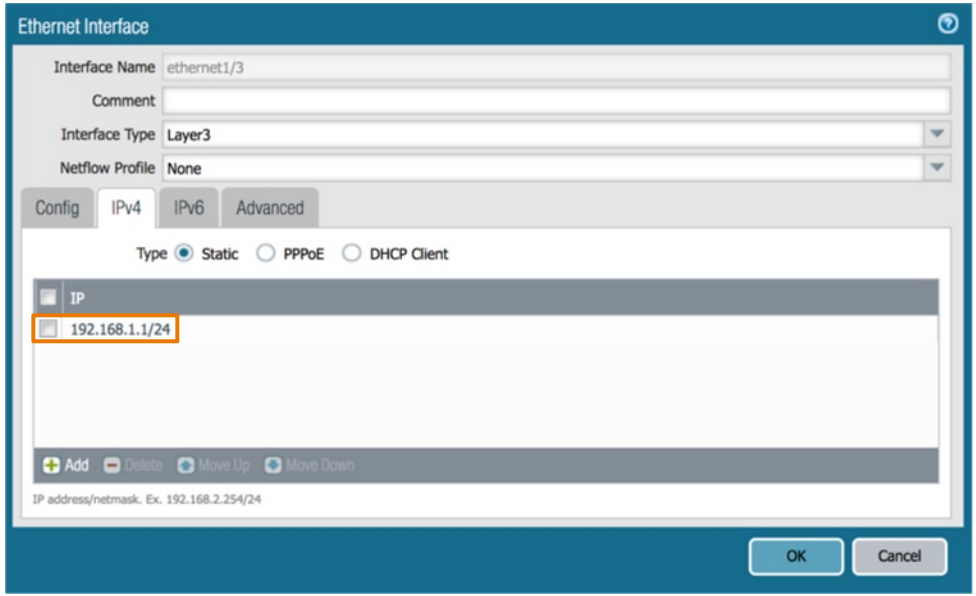
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



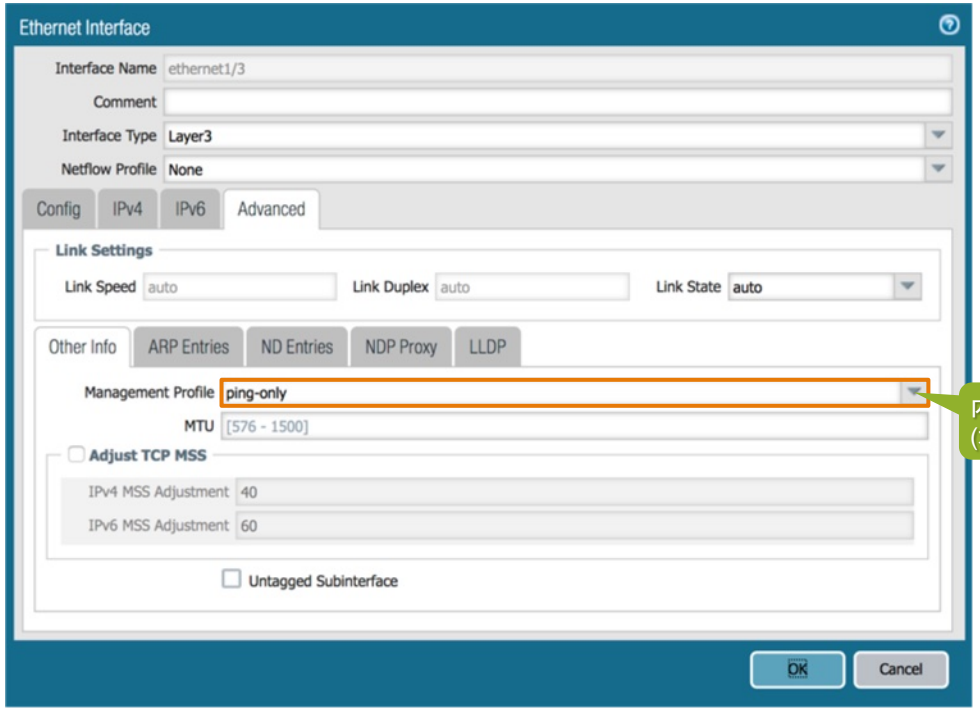
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク用インターフェイス設定

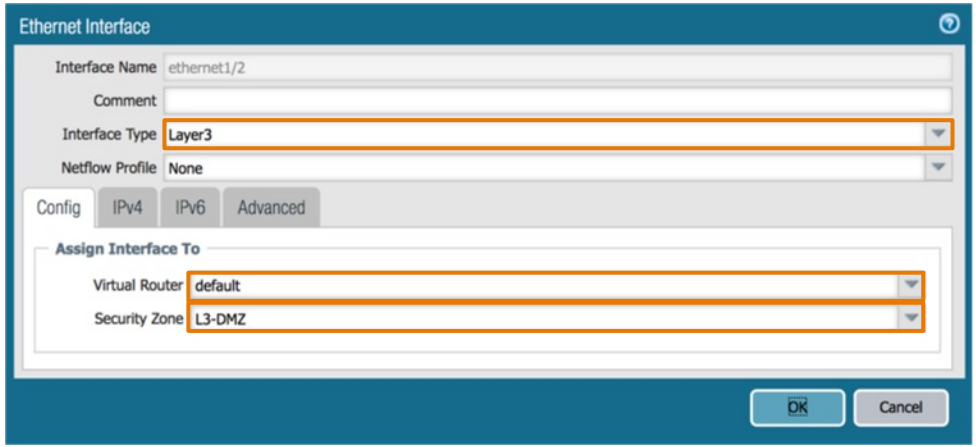
- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

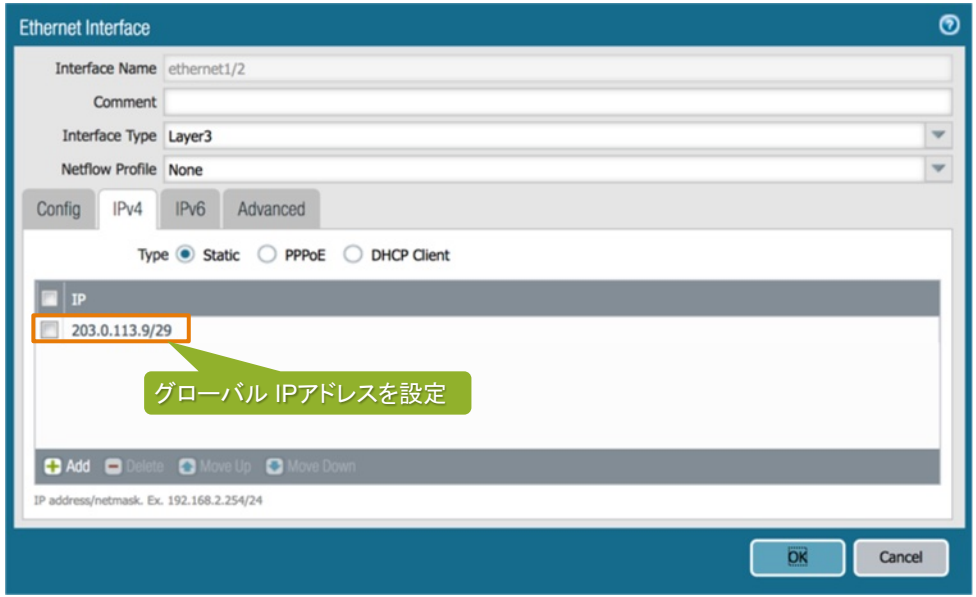
DMZネットワーク用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



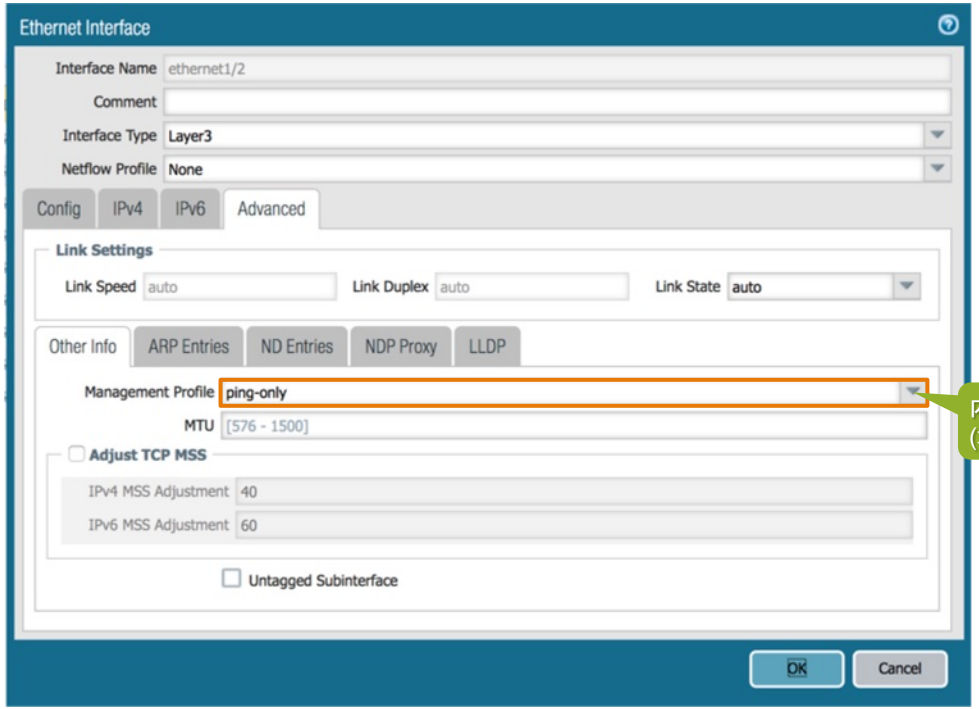
DMZネットワーク用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



DMZネットワーク用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

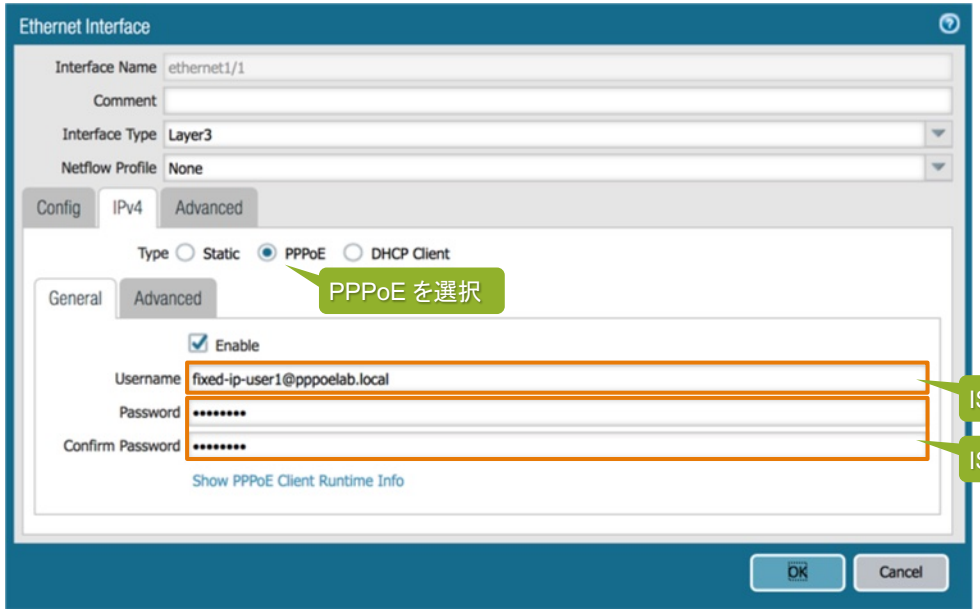
外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

新たに追加した仮想ルーターを指定

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

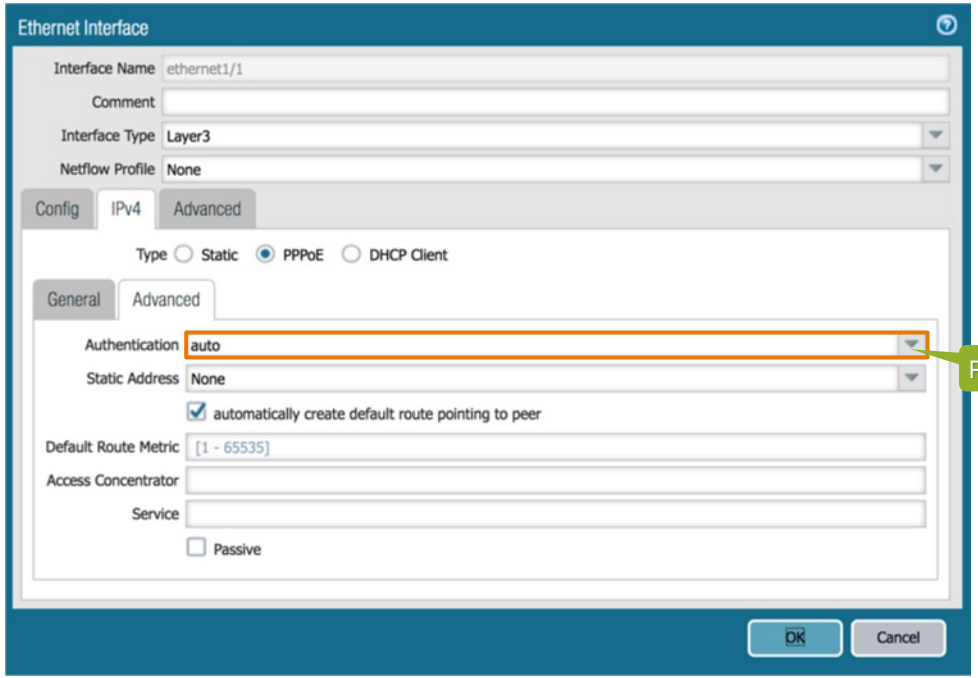


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

外部ネットワーク用インターフェイス設定

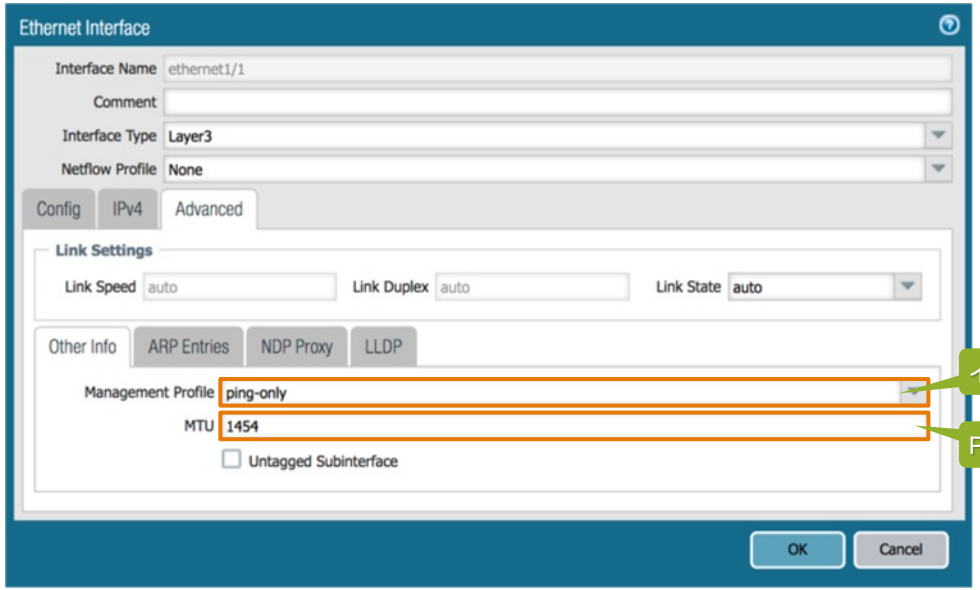
- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



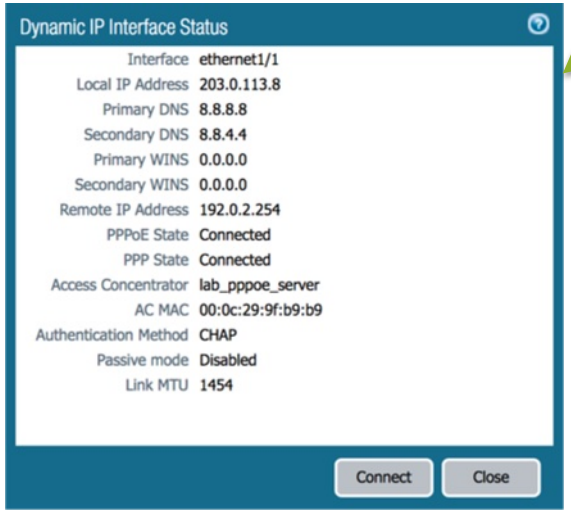
インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

ネットワークインターフェイス設定一覧

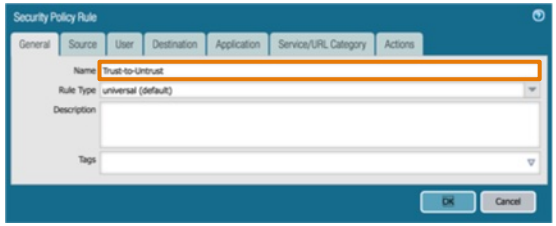
- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

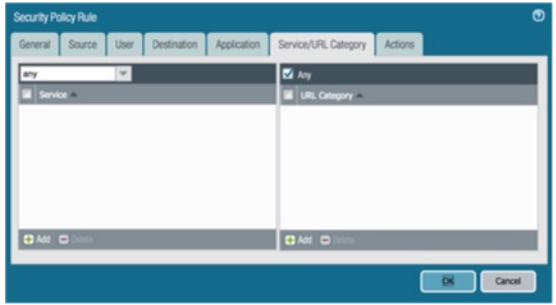
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone	Features
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	untrust-vr	Untagged	L3-Untrust	
ethernet1/2	Layer3	ping-only		203.0.113.9/29	default	Untagged	L3-DMZ	
ethernet1/3	Layer3	ping-only		192.168.1.1/24	default	Untagged	L3-Trust	

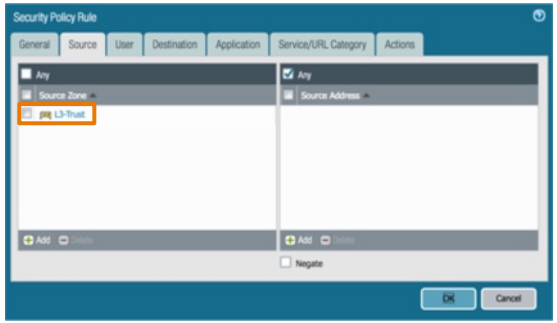


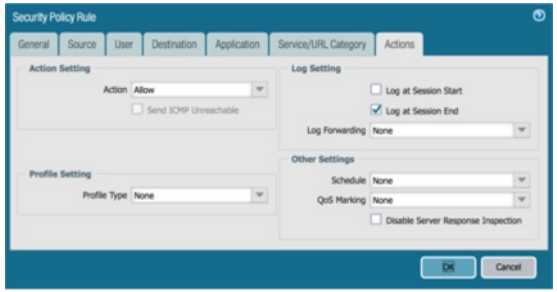
セキュリティポリシー設定

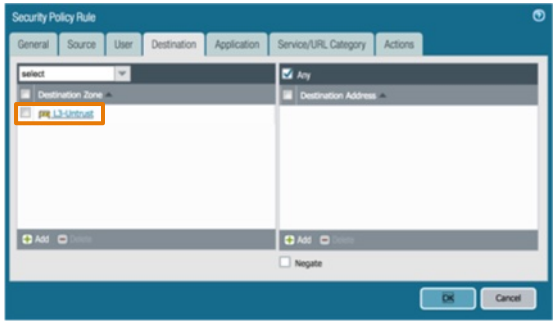
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)





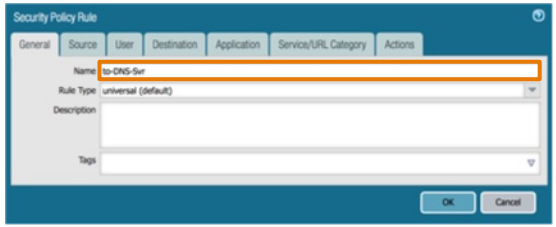


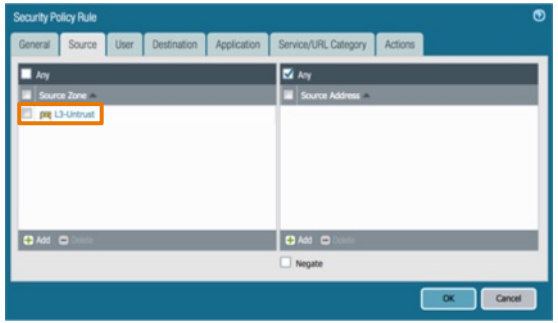


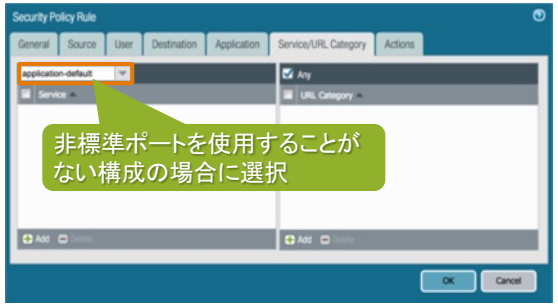


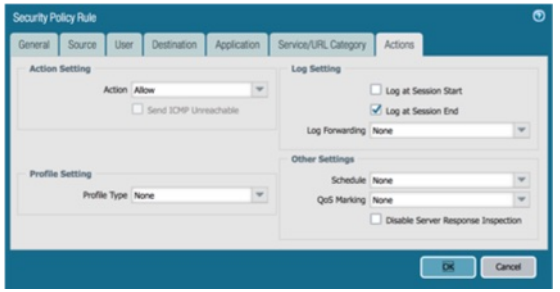
セキュリティポリシー設定

- 外部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



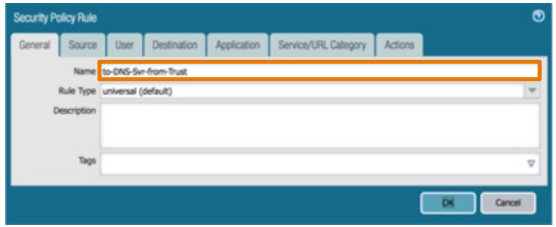


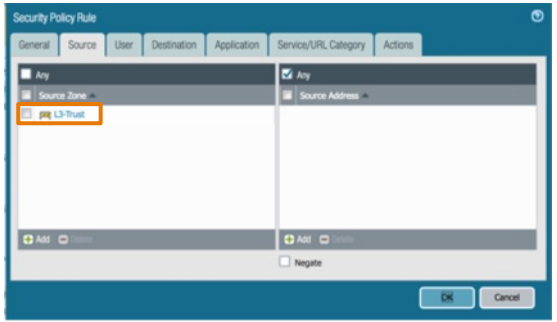


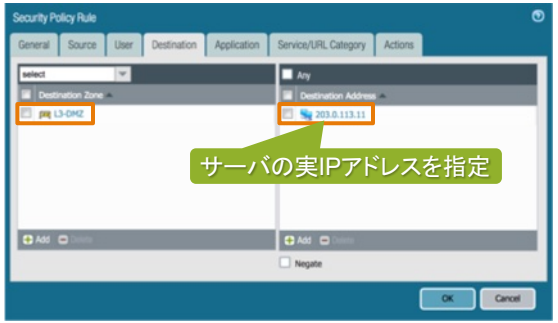


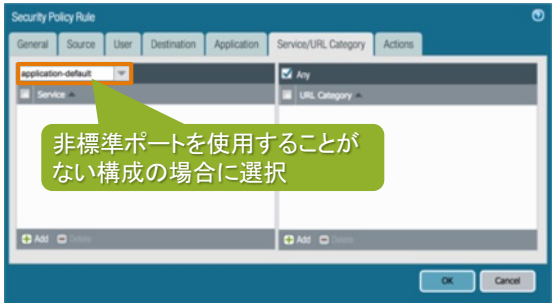
セキュリティポリシー設定

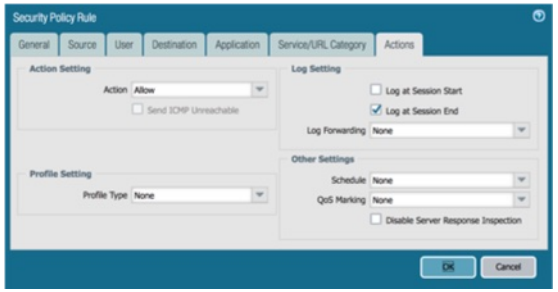
- 内部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)





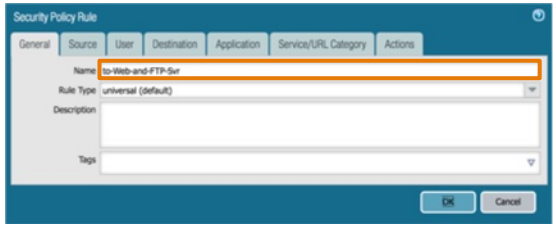


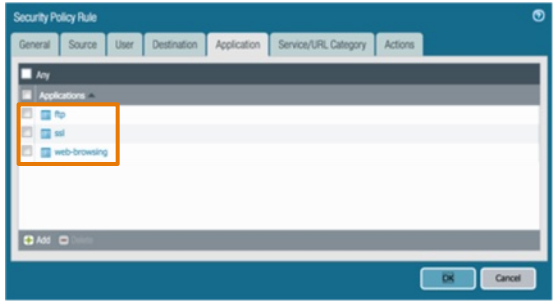


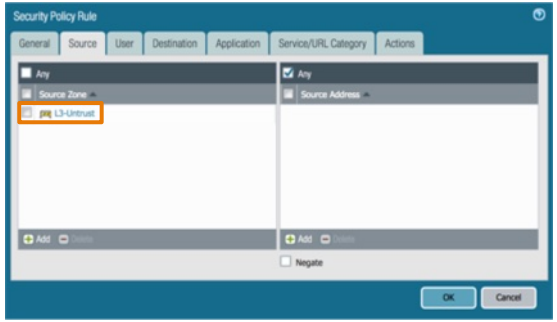


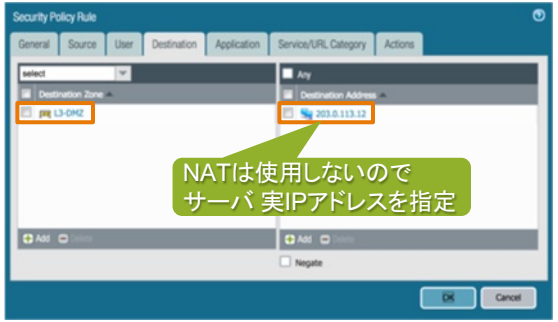
セキュリティポリシー設定

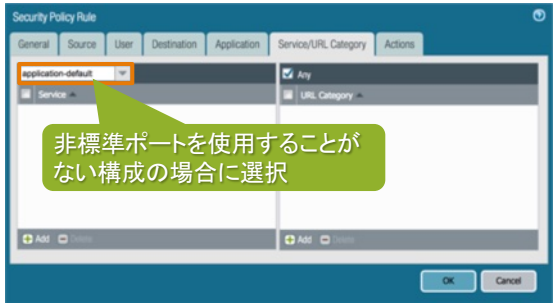
- 外部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)

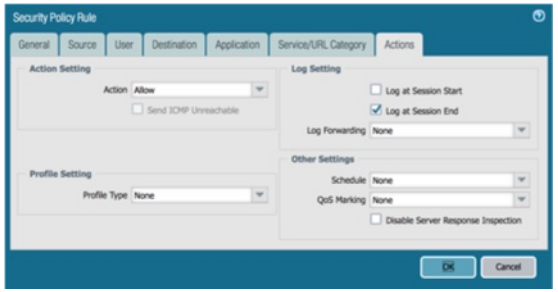






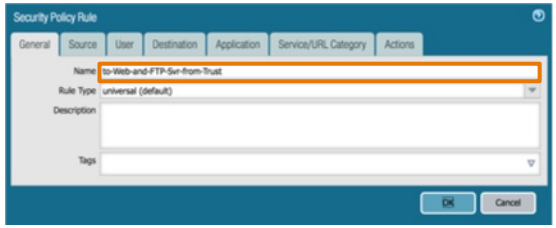


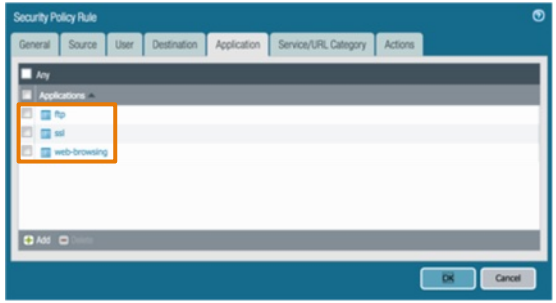


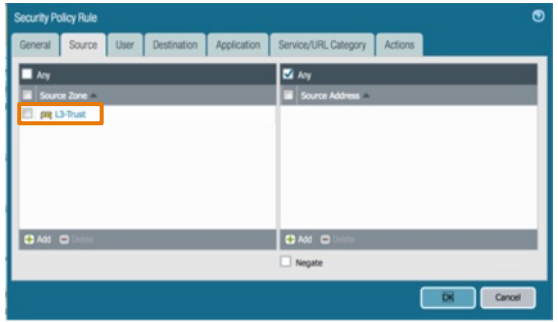


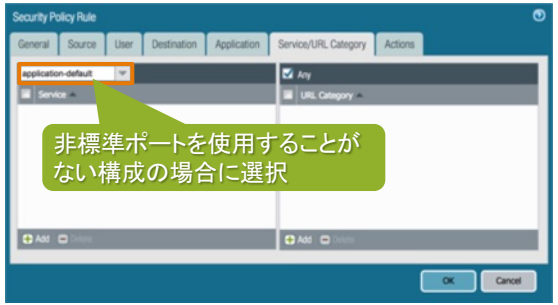
セキュリティポリシー設定

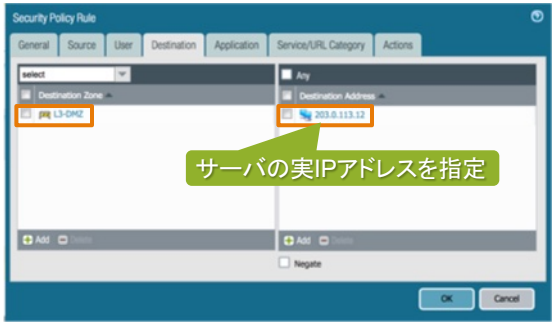
- 内部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)

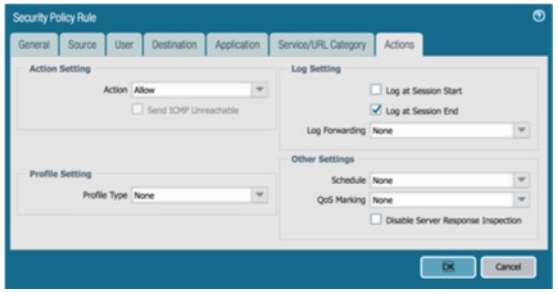






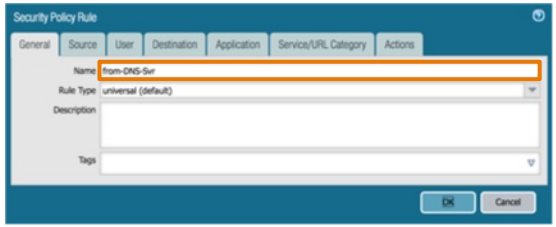


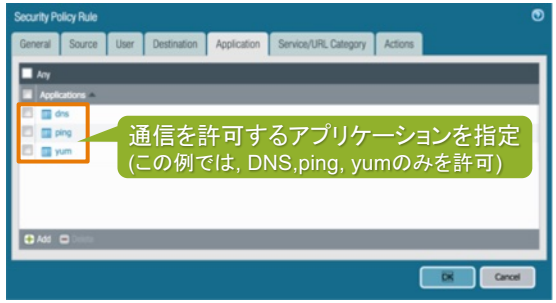


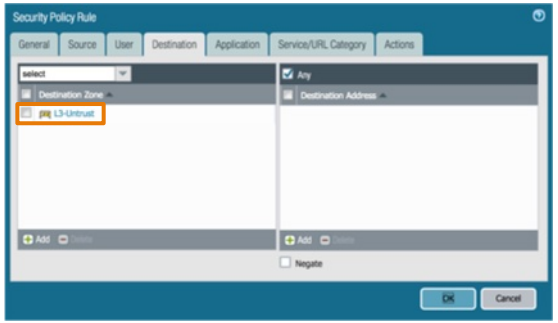


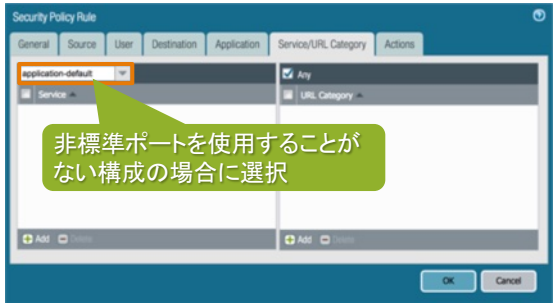
セキュリティポリシー設定

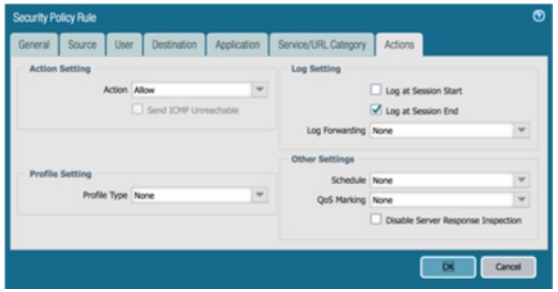
- DNSサーバ→外部向け通信用セキュリティポリシーの設定 (Policies > Security)





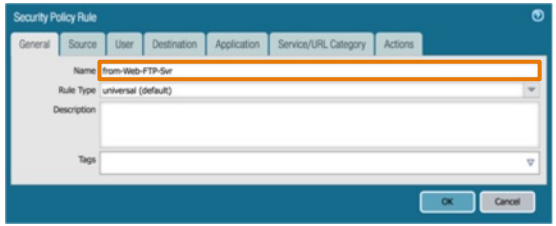


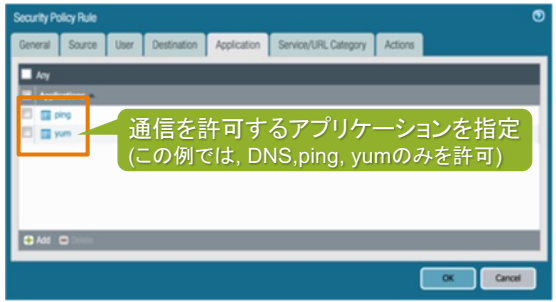


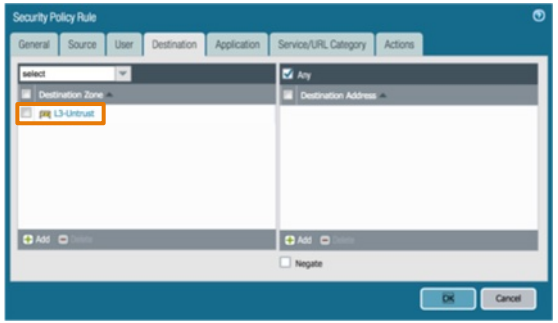


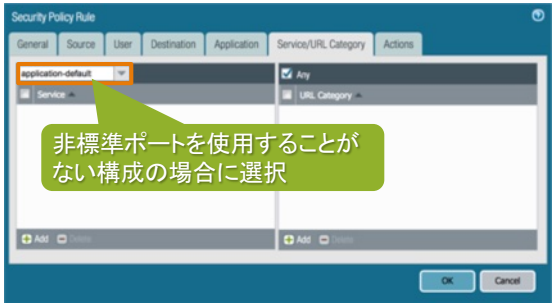
セキュリティポリシー設定

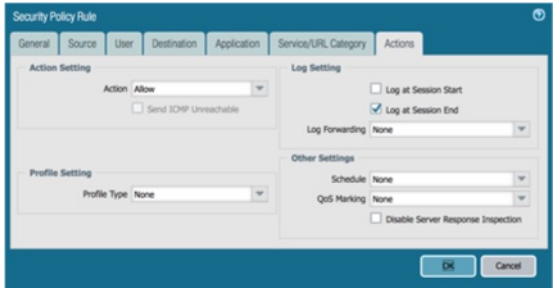
- Web/FTPサーバ→外部向け通信用セキュリティポリシーの設定 (Policies > Security)











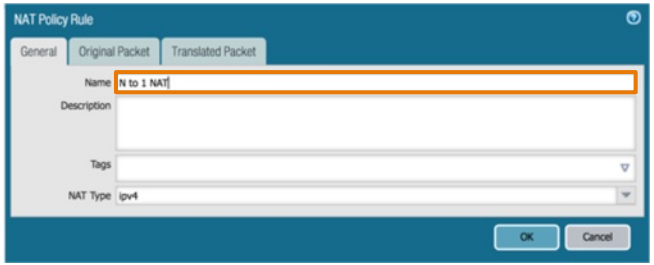
セキュリティポリシー設定一覧

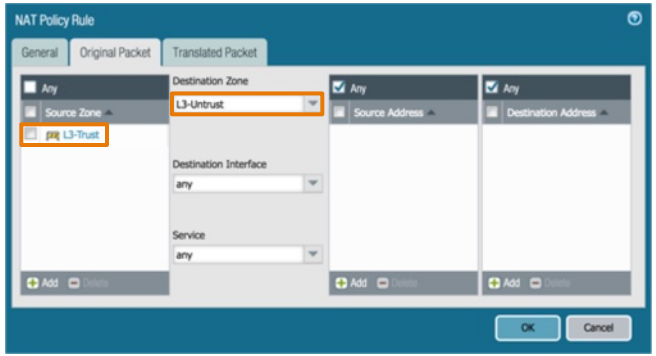
- セキュリティポリシー設定一覧 (Policies > Security)

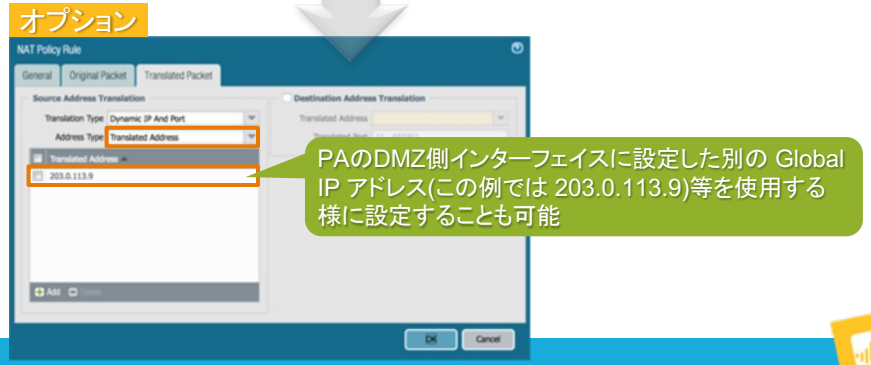
				Source			Destination						
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
2	to-DNS-Svr	none	universal	L3-Untrust	any	any	L3-DMZ	203.0.113.11	dns	application-default	Allow	none	
3	to-DNS-Svr-from-Trust	none	universal	L3-Trust	any	any	L3-DMZ	203.0.113.11	dns	application-default	Allow	none	
4	to-Web-and-FTP-Svr	none	universal	L3-Untrust	any	any	L3-DMZ	203.0.113.12	ftp ssl web-browsing	application-default	Allow	none	
5	to-Web-and-FTP-Svr-from-Trust	none	universal	L3-Trust	any	any	L3-DMZ	203.0.113.12	ftp ssl web-browsing	application-default	Allow	none	
6	from-DNS-Svr	none	universal	L3-DMZ	203.0.113.11	any	L3-Untrust	any	dns ping yum	application-default	Allow	none	
7	from-Web-FTP-Svr	none	universal	L3-DMZ	203.0.113.12	any	L3-Untrust	any	ping yum	application-default	Allow	none	
8	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
9	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)







NATポリシー設定一覧

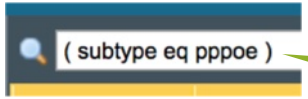
- NATポリシー設定一覧 (Policies > NAT)

	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

設定後のPPPoE 接続ログ・接続状態

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/26 07:27:34	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:17, IP Address negotiated:203.0.113.8
03/26 07:27:30	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1

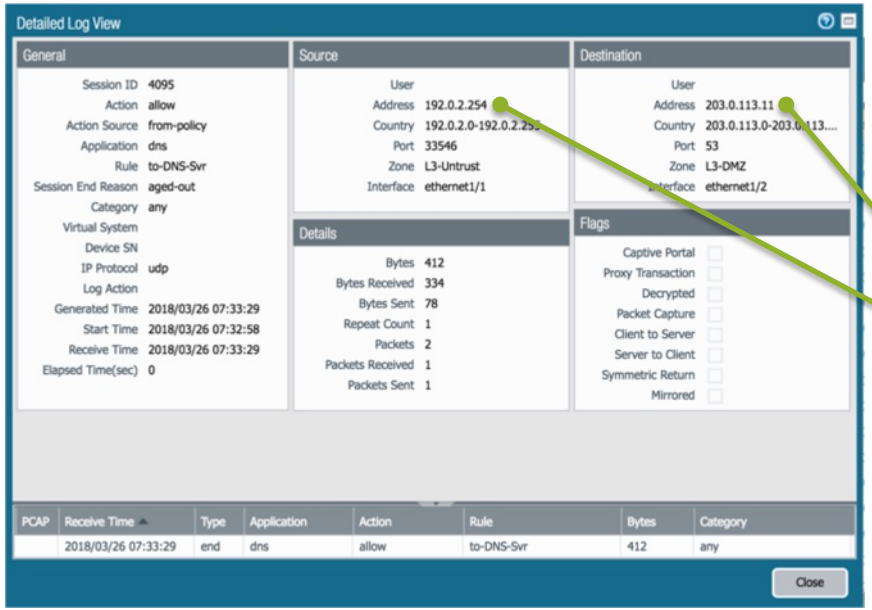


表示フィルタを使用することで必要なログを素早く確認することが可能

設定後のトラフィックログ例

- 外部からDMZ上のDNSサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 07:33:29	end	L3-Untrust	L3-DMZ	192.0.2.254	203.0.113.11	53	dns	any	allow	to-DNS-Svr	aged-out	412

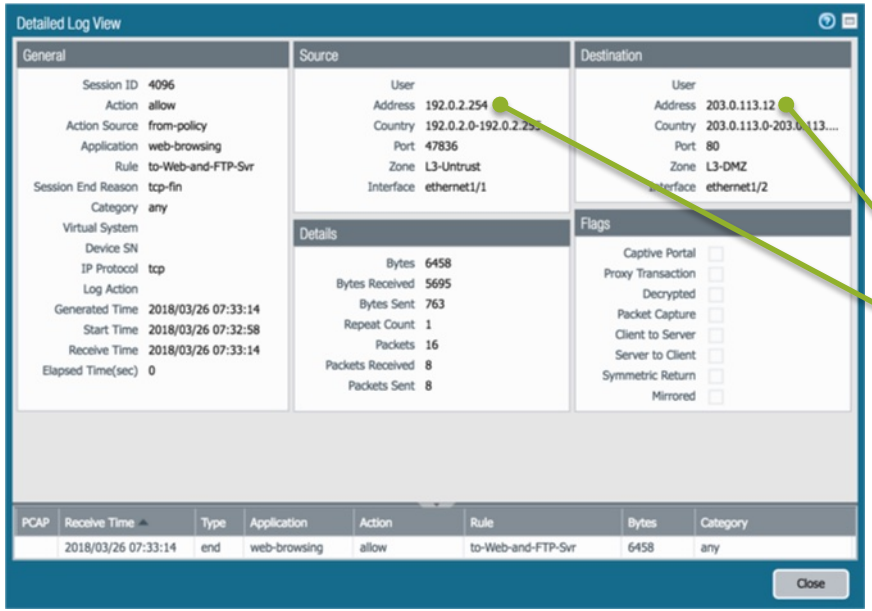


NATを使用しないので送信元 IPアドレスはオリジナルのまま

設定後のトラフィックログ例

- 外部からDMZ上のWeb/FTPサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 07:33:14	end	L3-Untrust	L3-DMZ	192.0.2.254	203.0.113.12	80	web-browsing	any	allow	to-Web-and-FTP-Svr	tcp-fin	6.5k

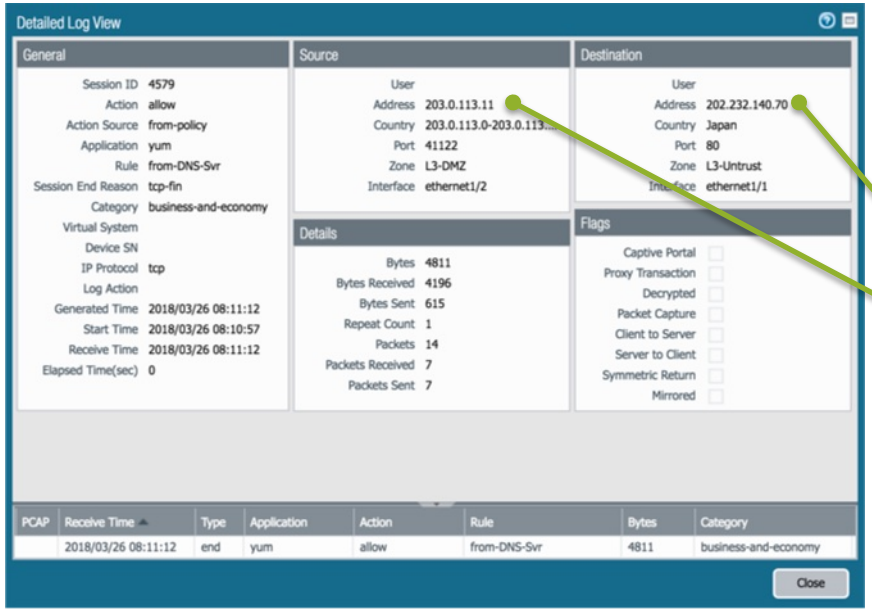


NATを使用しないので送信元 IPアドレスはオリジナルのまま

設定後のトラフィックログ例

- DMZ上のDNSサーバから外部側へ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 08:11:12	end	L3-DMZ	L3-Untrust	203.0.113.11	202.232.140.70	80	yum	business-and-economy	allow	from-DNS-Svr	tcp-fin	4.8k

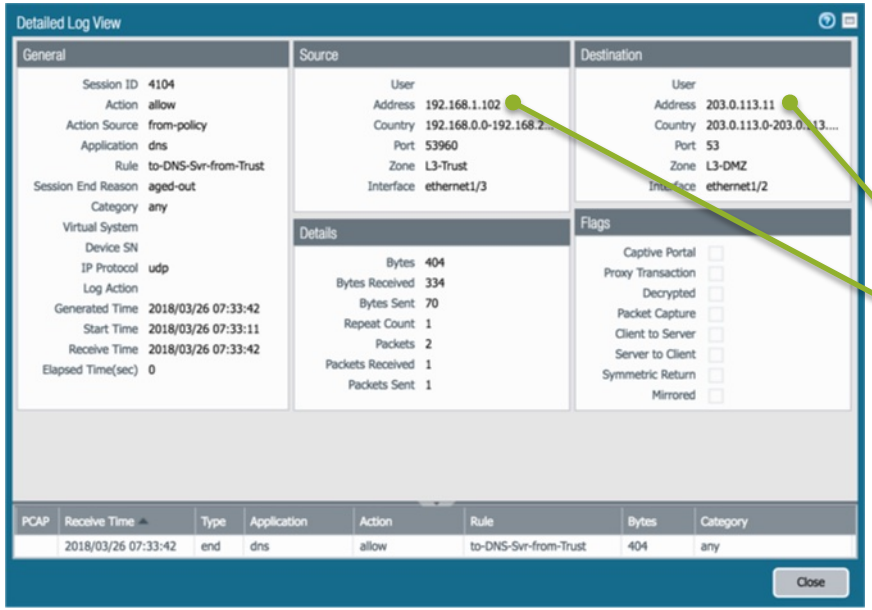


NATを使用しないので送信元 IPアドレスはオリジナルのまま

設定後のトラフィックログ例

- 内部からDMZ上のDNSサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 07:33:42	end	L3-Trust	L3-DMZ	192.168.1.102	203.0.113.11	53	dns	any	allow	to-DNS-Svr-from-Trust	aged-out	404

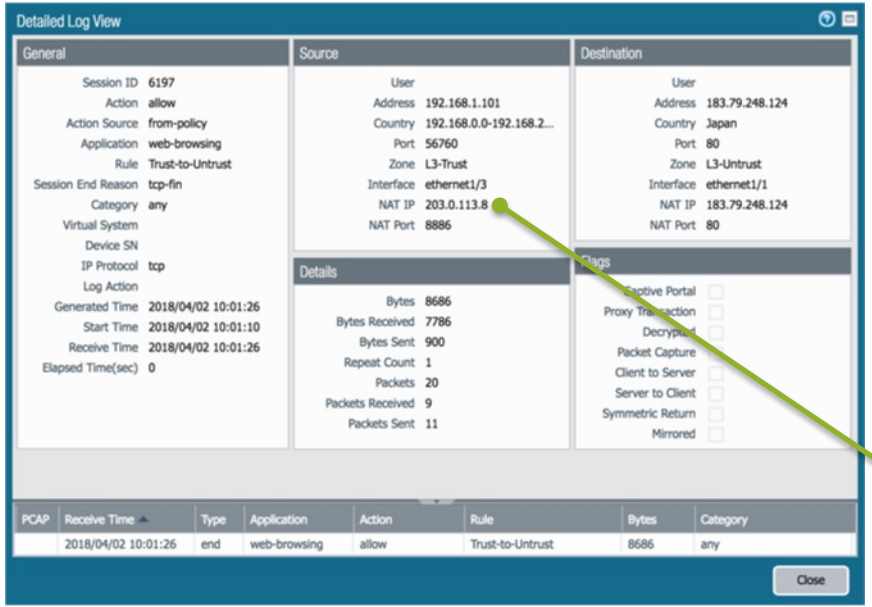


NATを使用しないので送信元 IPアドレスはオリジナルのまま

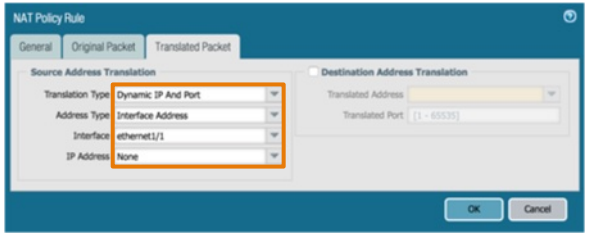
設定後のトラフィックログ例

- 内部からインターネットへ通信した場合のログ例1 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		04/02 10:01:26	end	L3-Trust	L3-Untrust	192.168.1.101	183.79.248.124	80	web-browsing	any	allow	Trust-to-Untrust	tcp-fin	8.7k



[該当NATポリシー設定の抜粋] ※参考

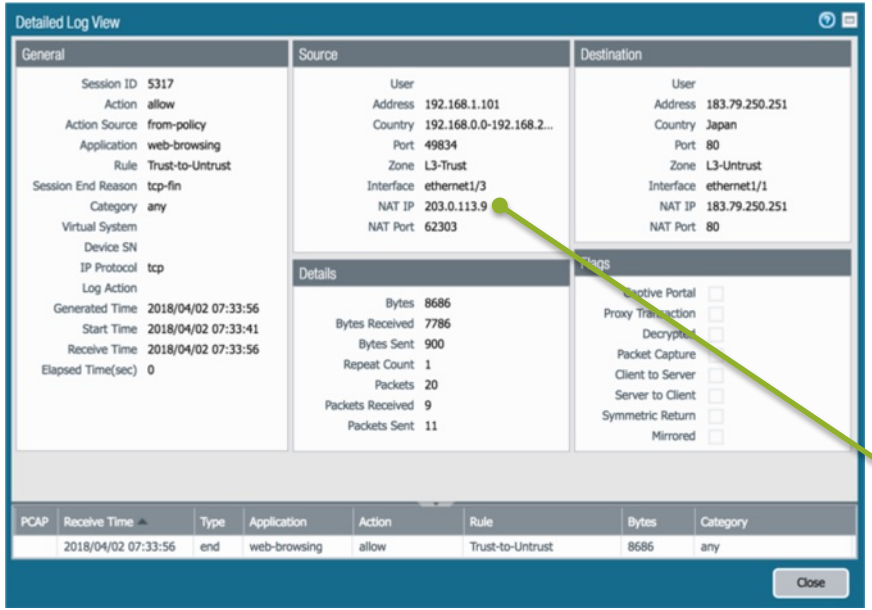


PPPoE インターフェイスに割り当てられたIPアドレス
(本例では8 IP LAN型構成のネットワークアドレス)に変換

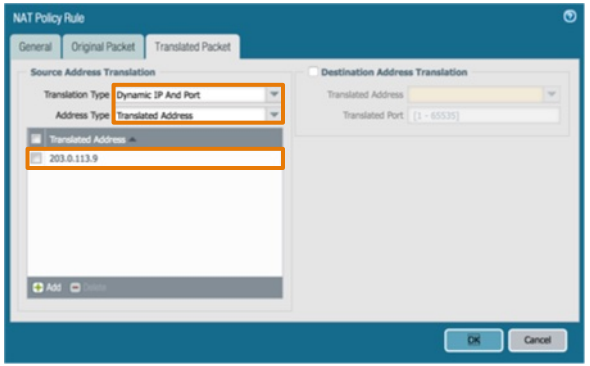
設定後のトラフィックログ例

- 内部からインターネットへ通信した場合のログ例2 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		04/02 07:33:56	end	L3-Trust	L3-Untrust	192.168.1.101	183.79.250.251	80	web-browsing	any	allow	Trust-to-Untrust	tcp-fin	8.7k



[該当NATポリシー設定の抜粋] ※参考

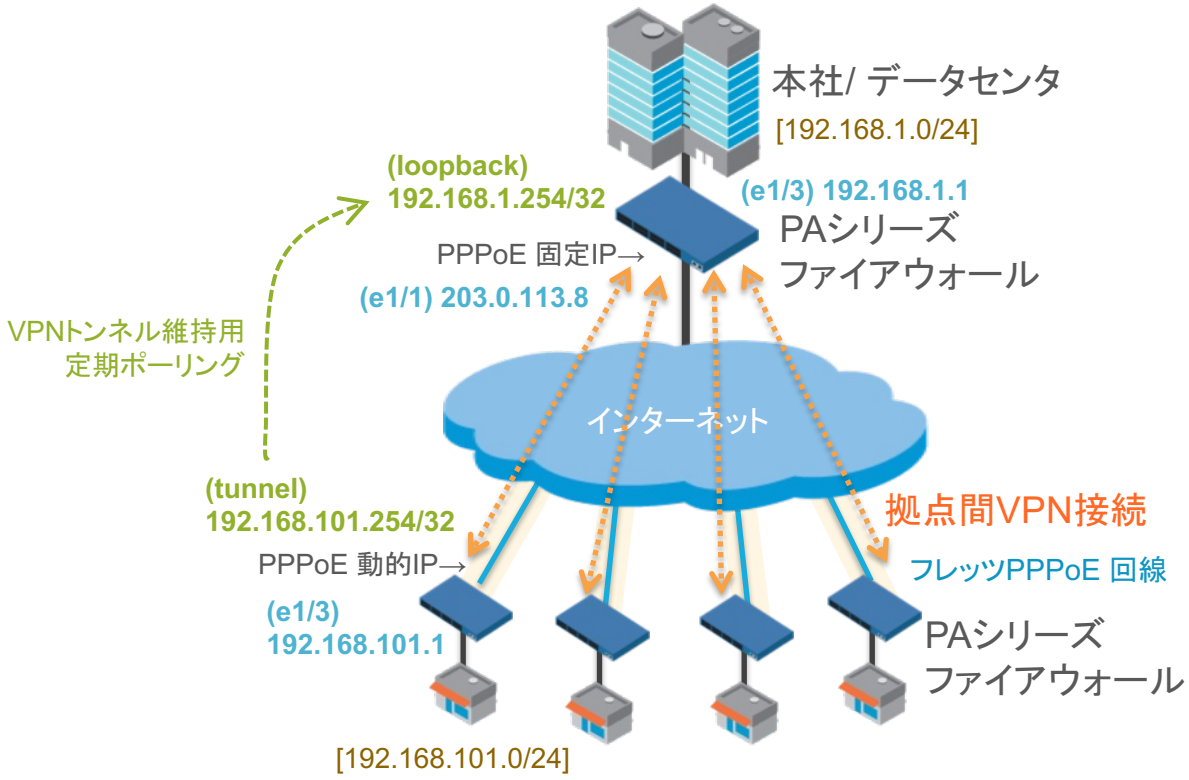


PAのDMZ LAN インターフェイスに設定された IPアドレス
(本例では8 IP LAN型構成の1つめのホストアドレス)に変換

PPPoE 設定例 4

PPPoE回線を使用したインターネット接続と
拠点間VPN接続

システム構成：



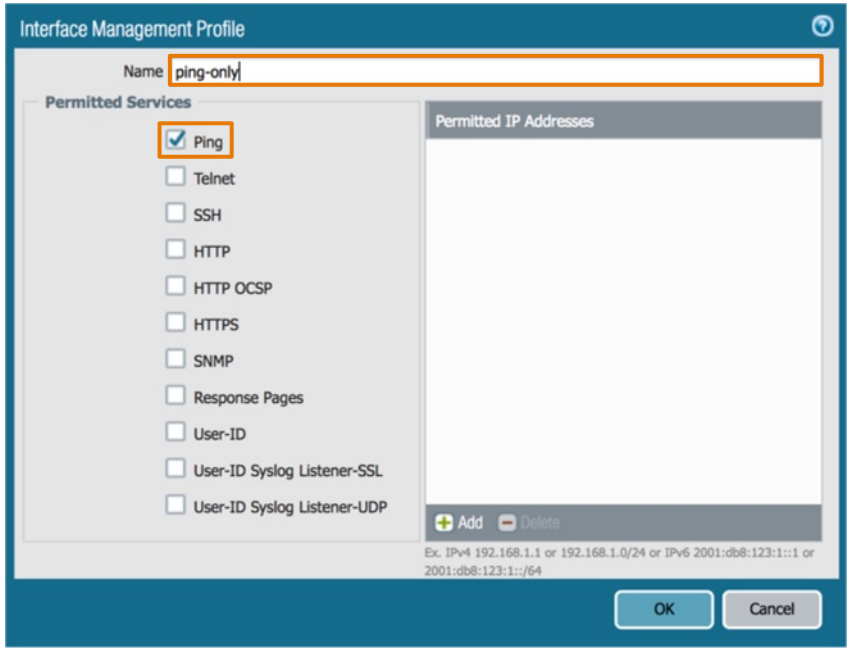
コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE関連	・MTU 値を必ず変更する。（例：1454） ・PPPoE 認証方式はデフォルトのままで問題なし。 ・固定IPアドレスサービスを使用する場合も PPPoE を有効にしているインターフェイスに明示的に設定する必要はない。（設定しても問題はない）
その他	・動的IPアドレスを使用する拠点側からの通信がない場合でもVPN接続を維持するため（本社側からの監視やリモートメンテナンスなどの目的）拠点側PAにおいて IPSec トンネルモニタ機能を使用。VPN常時接続の必要性がない場合や拠点側からの通信が定常的に発生する構成の場合はこの設定は不要。

☆実環境においては、各種脅威防御やURLフィルタリング WildFireなど、重要なセキュリティ機能を必ず設定・ご利用下さい。

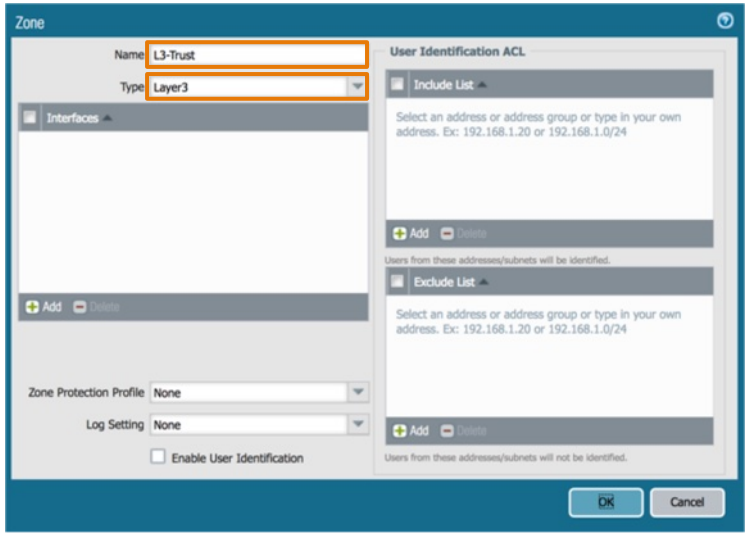
センター側：インターフェイス管理アクセス設定

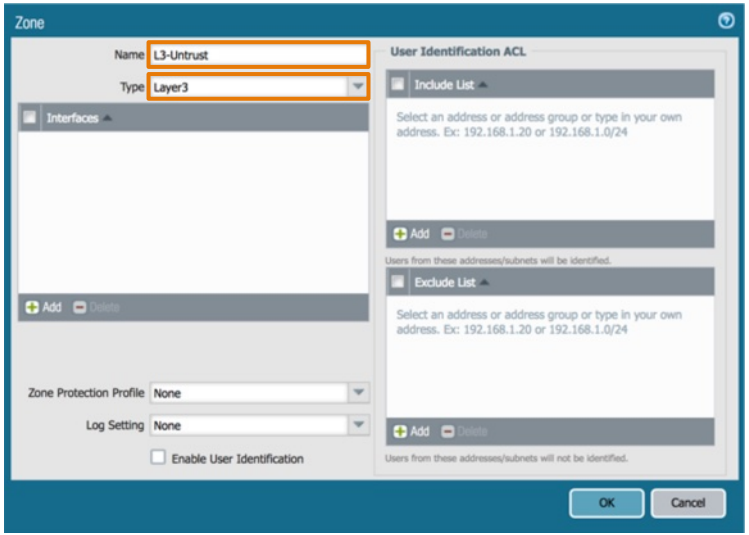
- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)



センター側：セキュリティゾーン設定

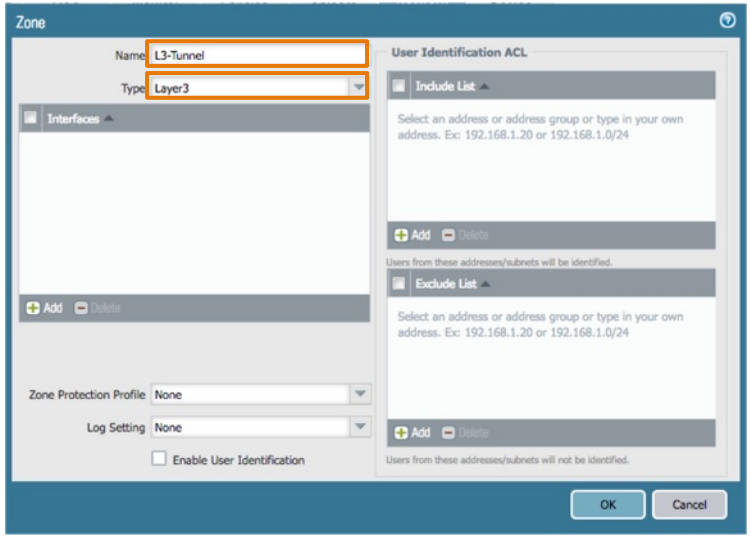
- 内部ネットワーク用、外部ネットワーク(インターネット)用セキュリティゾーンを作成 (Network > Zones)





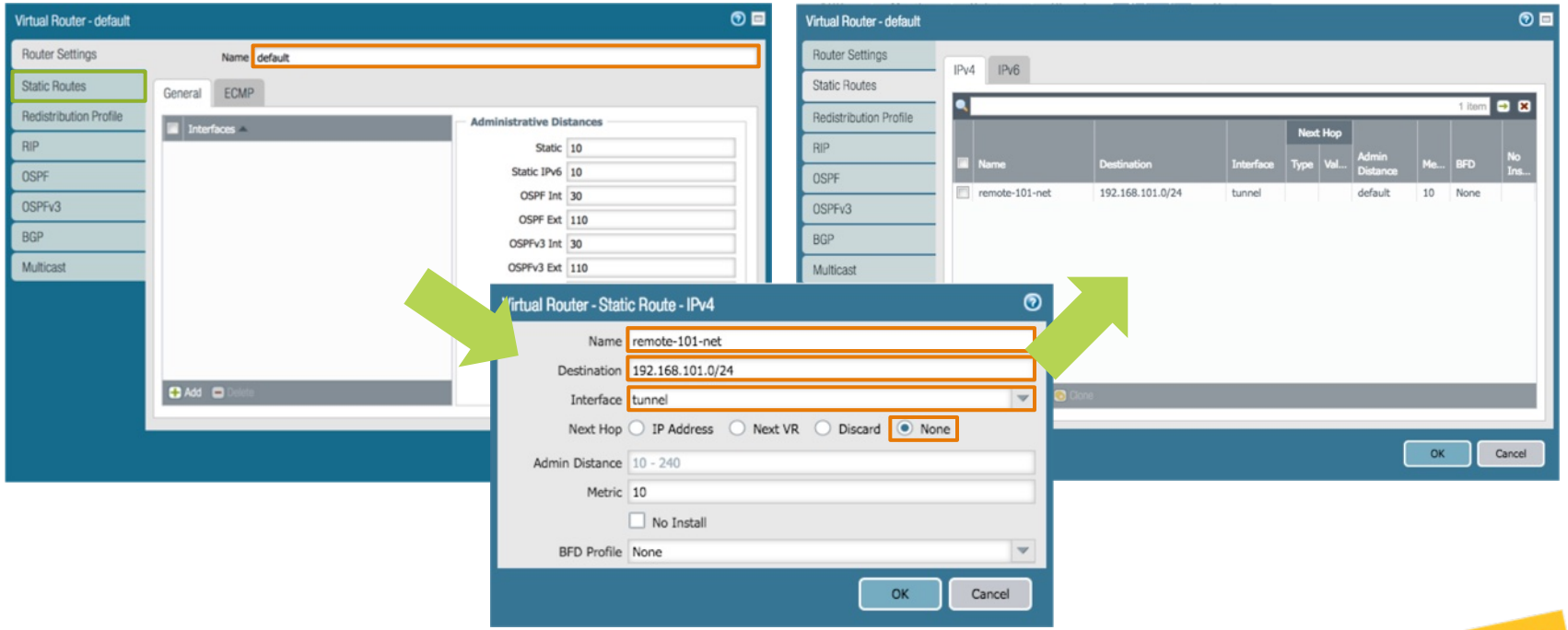
センター側：セキュリティゾーン設定

- VPN通信用セキュリティゾーンを作成
(Network > Zones)



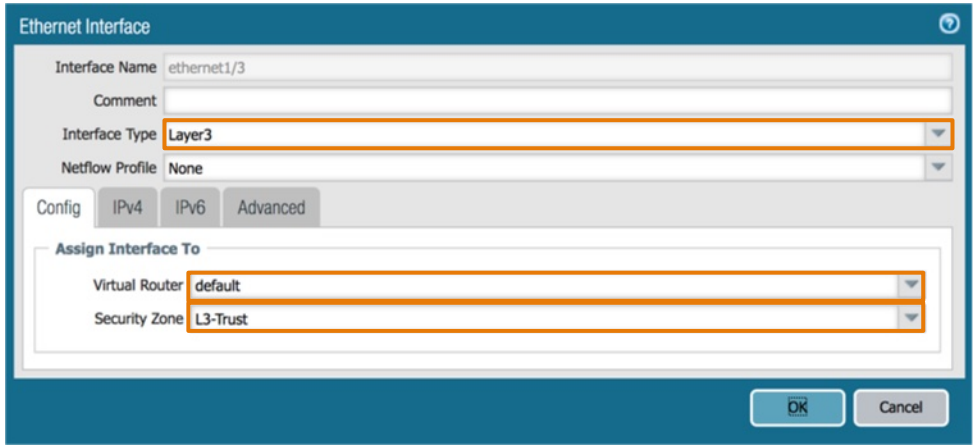
センター側：仮想ルーター設定

- デフォルト仮想ルーター(default)に対して(VPN経由) 拠点側の内部ネットワーク向けのStatic Routeを追加 (Network > Virtual Routers > default > Static Routes > Add)



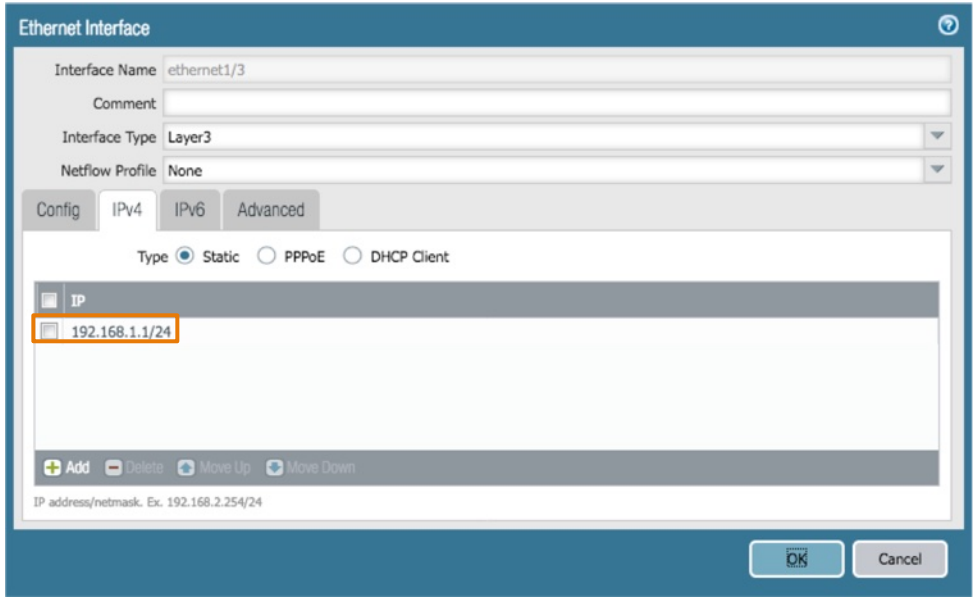
センター側：内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



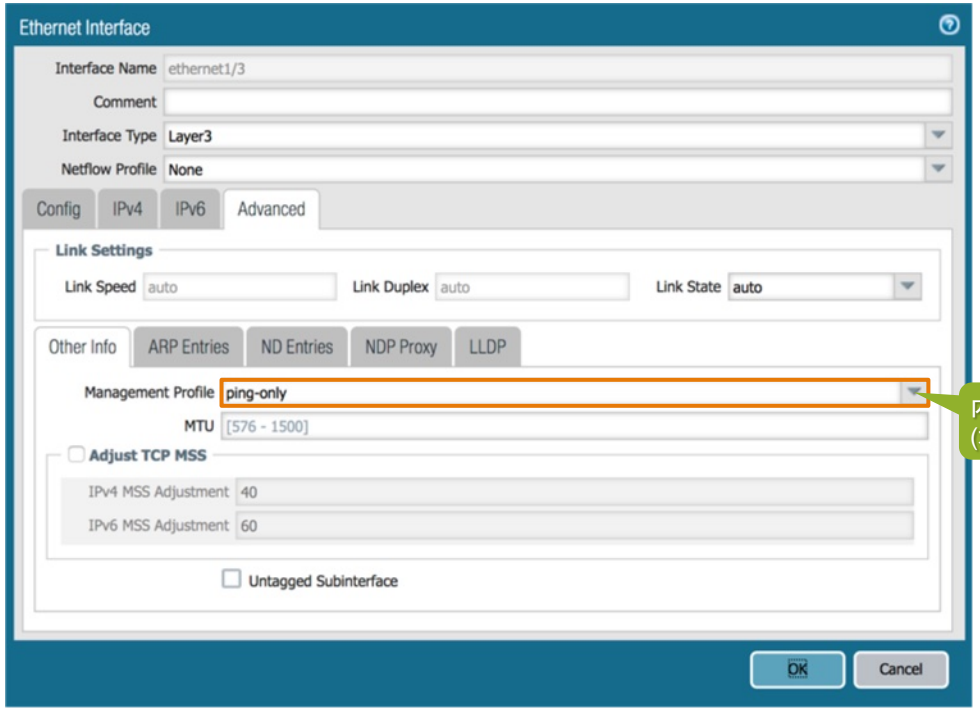
センター側：内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



センター側：内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



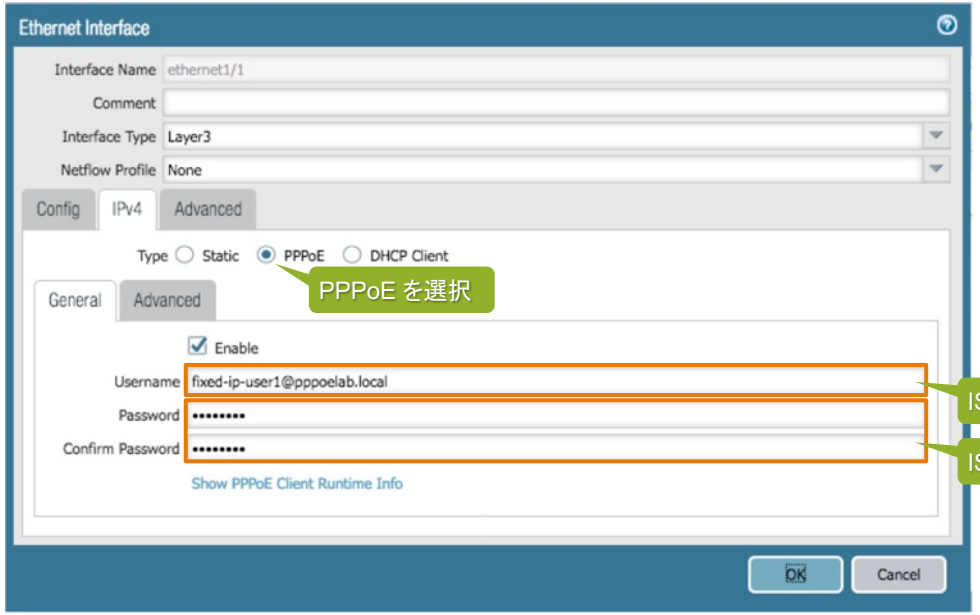
内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

センター側：外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

センター側：外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

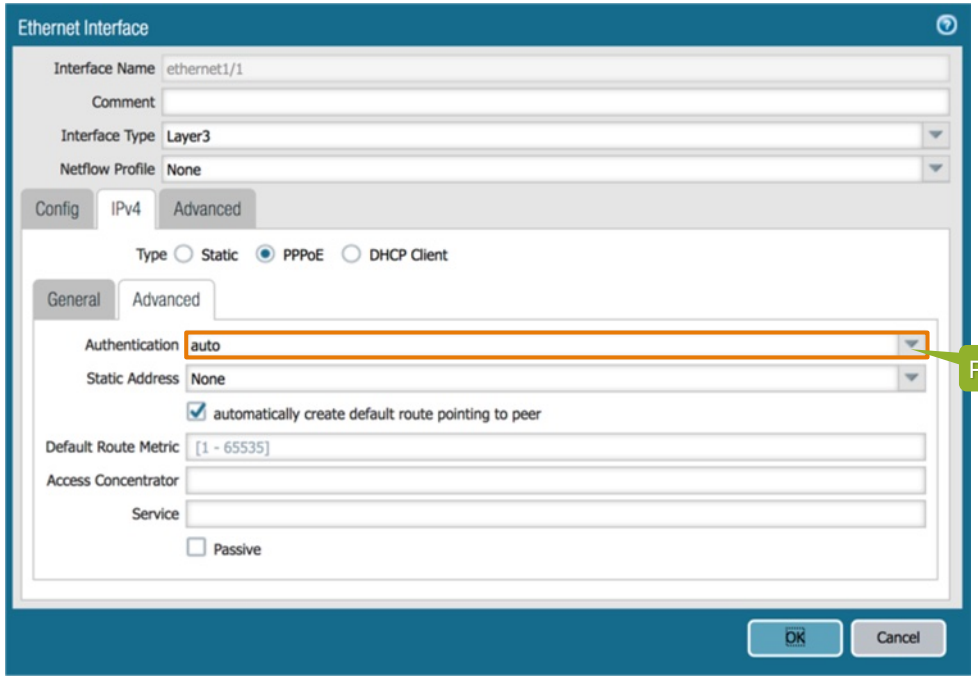


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

センター側：外部ネットワーク用インターフェイス設定

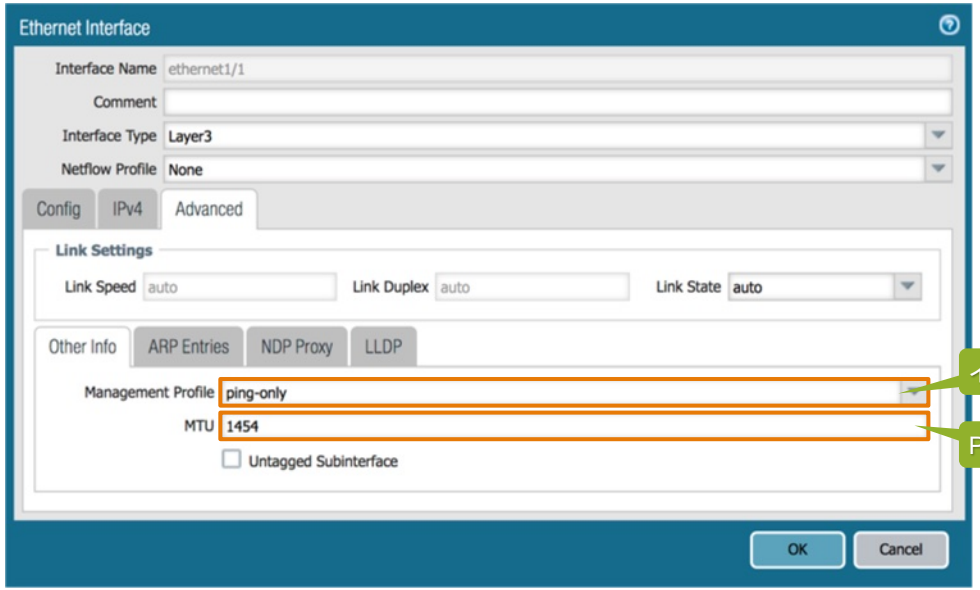
- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

センター側：外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

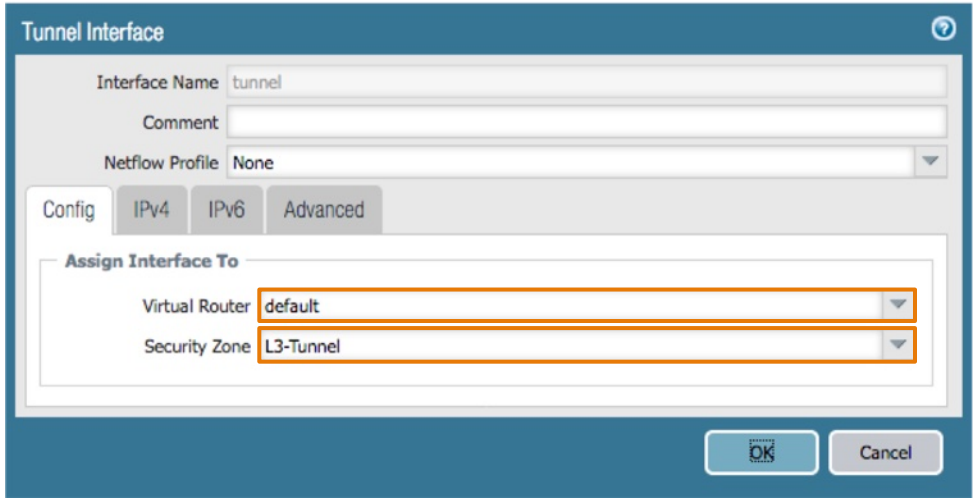


インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

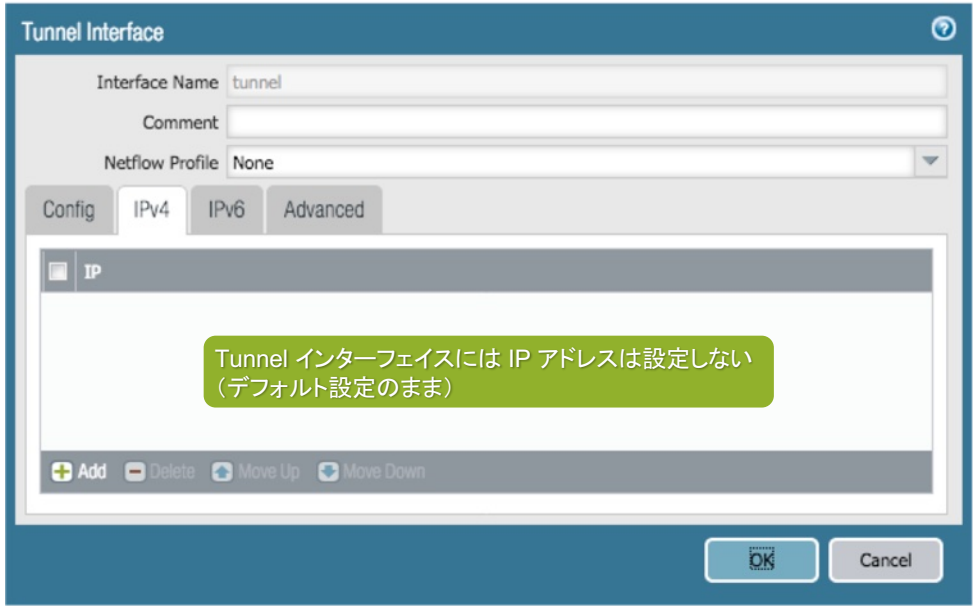
センター側：VPN用論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



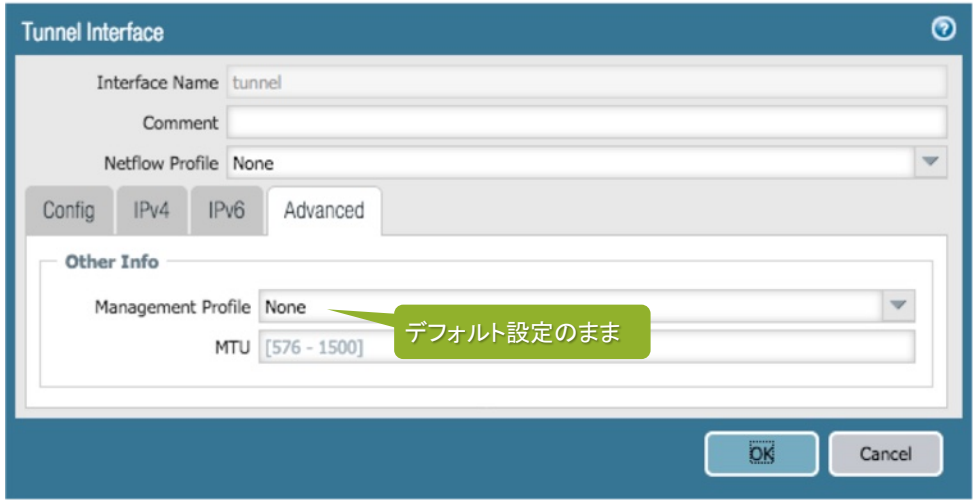
センター側：VPN用論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



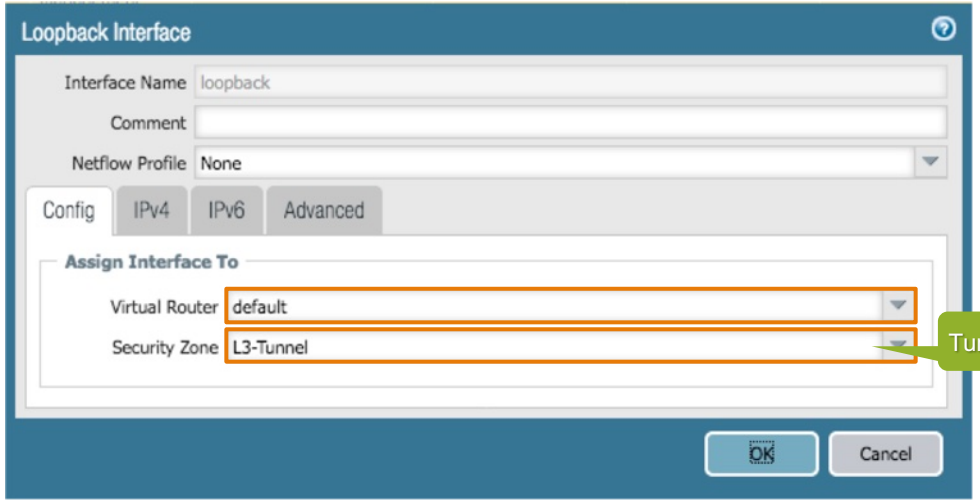
センター側：VPN用論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



センター側：VPN接続維持用論理インターフェイス設定

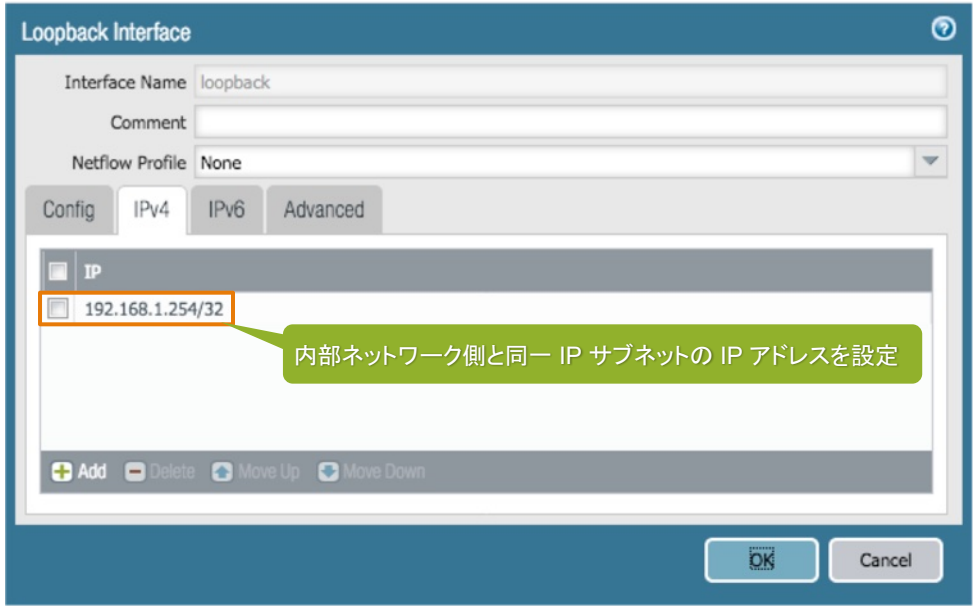
- loopback インターフェイスの設定 (Network > Interfaces > Loopback)



Tunnel インターフェイスと同一のセキュリティゾーンにマッピング

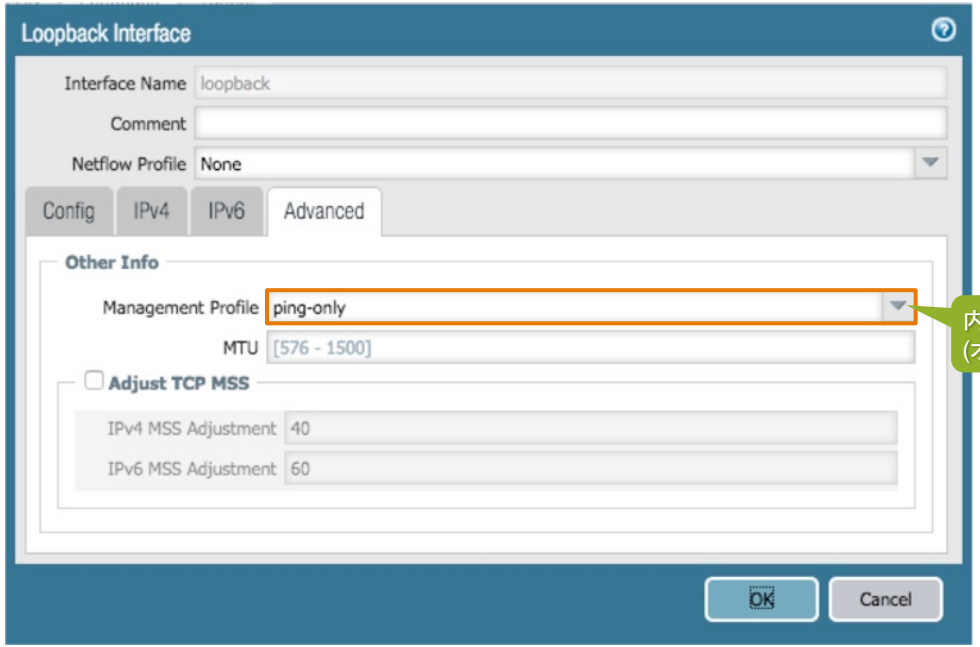
センター側：VPN接続維持用論理インターフェイス設定

- loopback インターフェイスの設定 (Network > Interfaces > Loopback)



センター側：VPN接続維持用論理インターフェイス設定

- loopback インターフェイスの設定 (Network > Interfaces > Loopback)



内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

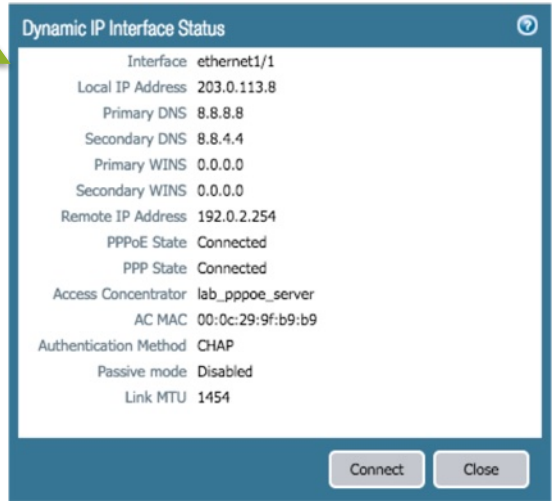
センター側：ネットワークインターフェイス設定一覧

- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	default	Untagged	none	L3-Untrust		
ethernet1/2				none	none	Untagged	none	none		
ethernet1/3	Layer3	ping-only		192.168.1.1/24	default	Untagged	none	L3-Trust		

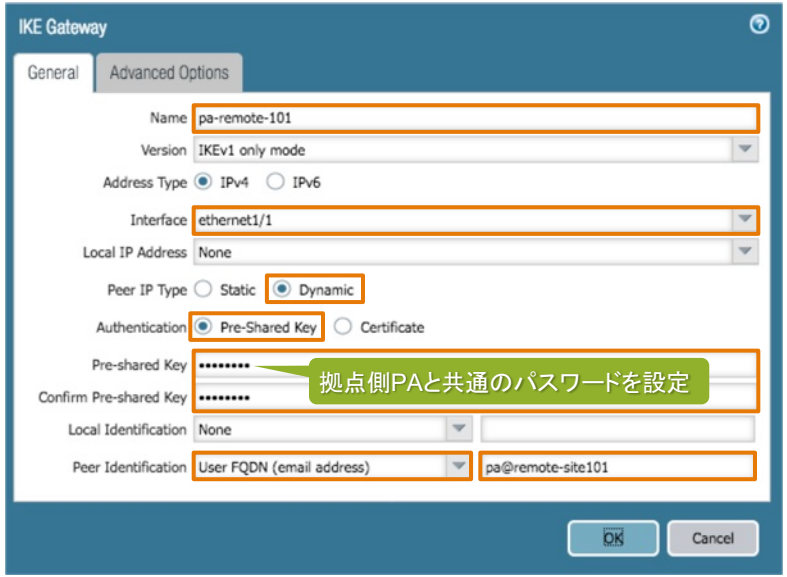
Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	default	L3-Tunnel		

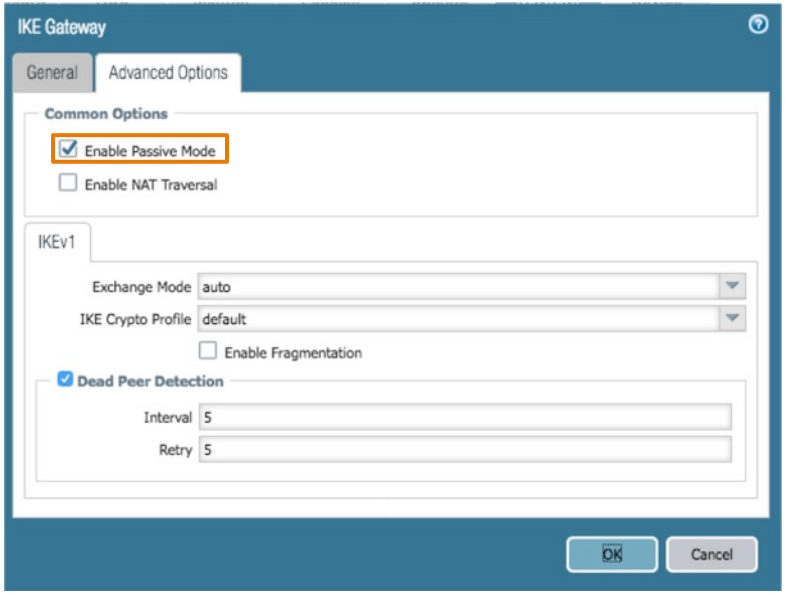
Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
loopback	ping-only	192.168.1.254/32	default	L3-Tunnel		



センター側：VPN接続用 IPSec IKE ゲートウェイ設定

- IKE Gateway (Network > Network Profiles > IKE Gateways)

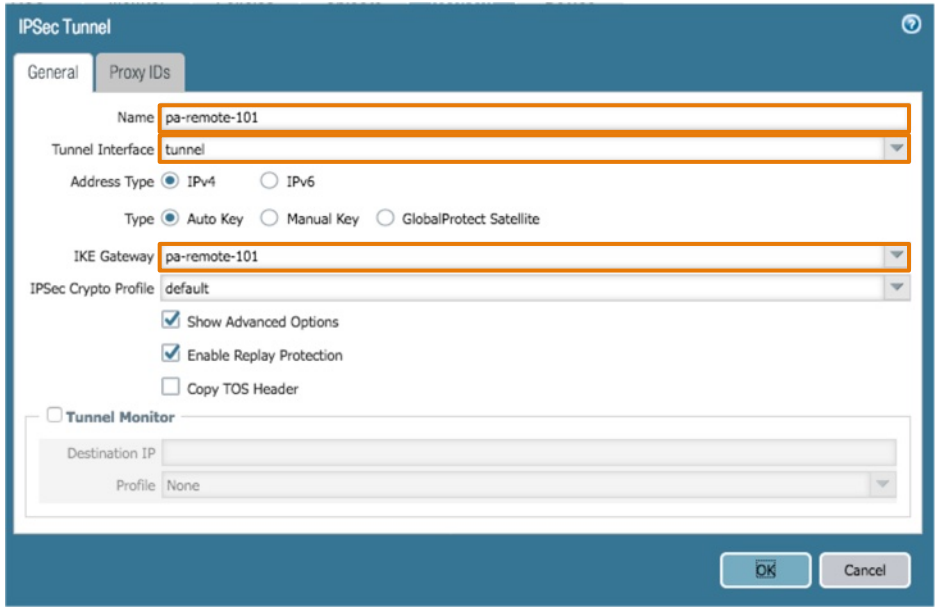




		Local Address		Peer ID		Local ID			IKE Advanced Options					
Name	Peer Address	Interface	IP	ID	Type	ID	Type	Version	Mode	Passive Mode	NAT Traversal	Crypto Profile	DPD	Liveness
pa-remote-101		ethernet1/1		pa@remote-site101	User FQDN (email address)			ikev1	auto	☑	☐	default	enabled/default/default	

センター側：VPN接続用 IPSec トンネル設定

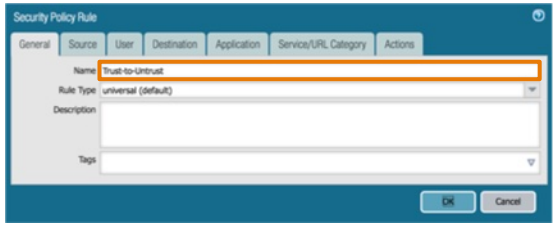
- IPSec Tunnel (Network > IPSec Tunnels)

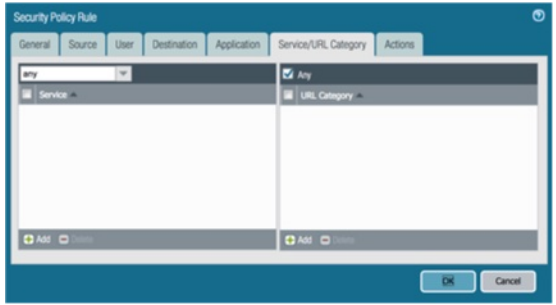


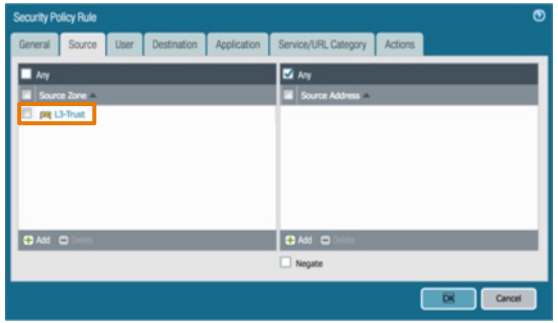
	Name	Status	Type	IKE Gateway/Satellite				Tunnel Interface				
				Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
	pa-remote-101	Tunnel Info	Auto Key	ethernet1/1		dynamic	IKE Info	tunnel	default (Show Routes)	vsys1	L3-Tunnel	

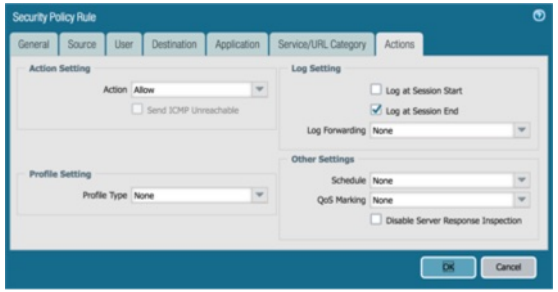
センター側：セキュリティポリシー設定

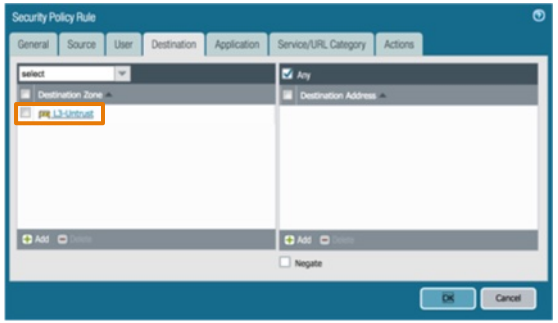
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)





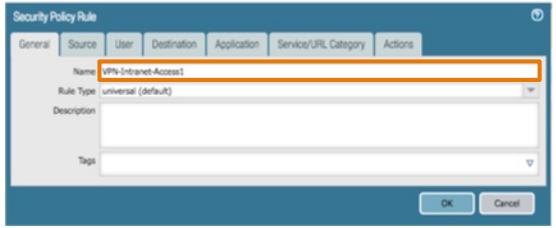


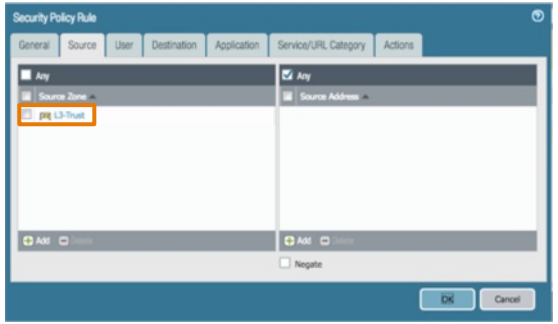


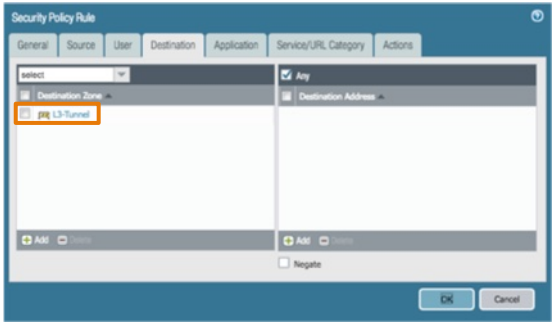


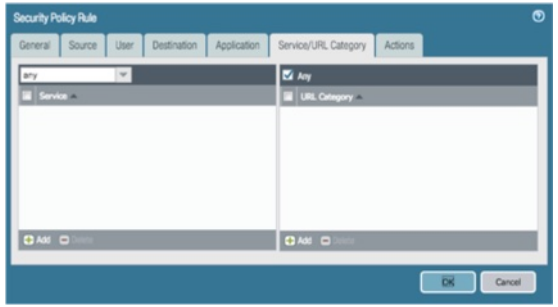
センター側：セキュリティポリシー設定

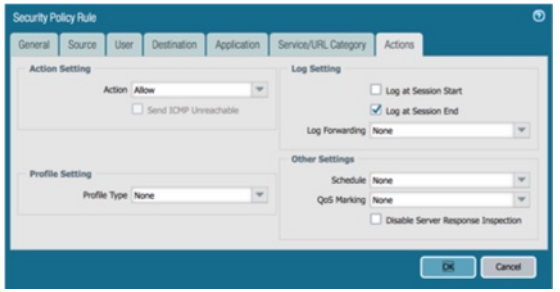
- リモート拠点向けVPN通信用セキュリティポリシーの設定1 (Policies > Security)





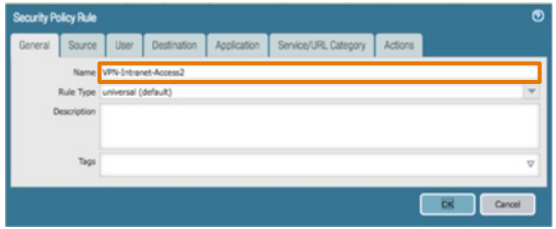


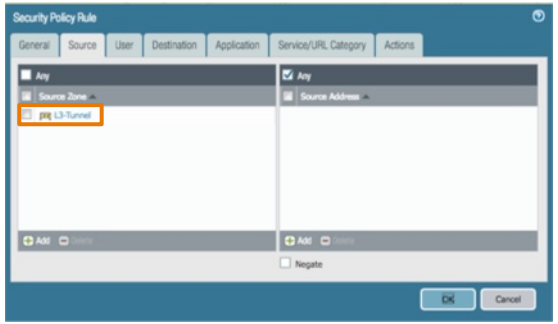


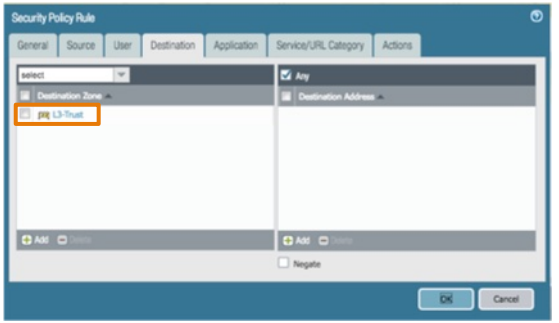


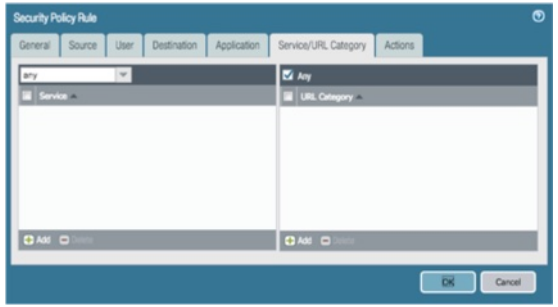
センター側：セキュリティポリシー設定

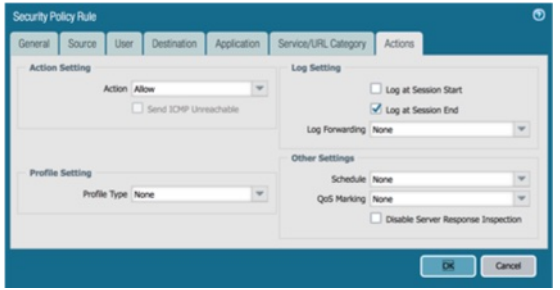
- リモート拠点向けVPN通信用セキュリティポリシーの設定2 (Policies > Security)











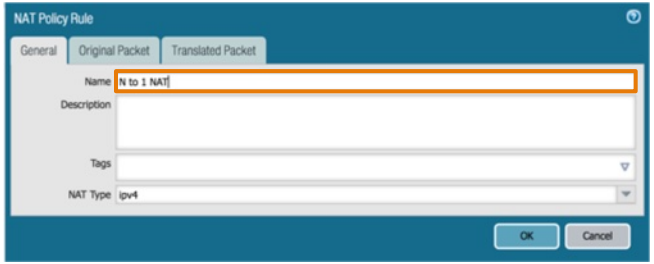
センター側：セキュリティポリシー設定一覧

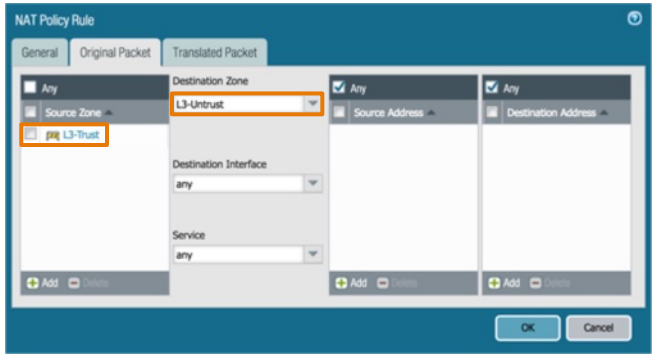
- セキュリティポリシー設定一覧 (Policies > Security)

				Source			Destination						
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
2	VPN-Intranet-Access1	none	universal	L3-Trust	any	any	L3-Tunnel	any	any	any	Allow	none	
3	VPN-Intranet-Access2	none	universal	L3-Tunnel	any	any	L3-Trust	any	any	any	Allow	none	
4	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

センター側：NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)





IPアドレスは指定しなくて良い
(インターフェイス に割当てられた
IPアドレスが自動的に使われる)

センター側：NATポリシー設定一覧

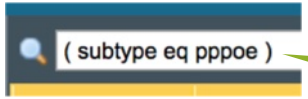
- NATポリシー設定一覧 (Policies > NAT)

	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

センター側：設定後の**PPPoE** 接続ログ

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/26 15:17:46	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:1, IP Address negotiated:203.0.113.8
03/26 15:17:42	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1



表示フィルタを使用することで必要なログを素早く確認することが可能

センター側：設定後のVPN 接続ログ

- VPN接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/26 15:31:54	vpn	informational	ike-config-p2-success		IKE daemon configuration load phase-2 succeeded.
03/26 15:31:50	vpn	informational	ike-config-p1-success		IKE daemon configuration load phase-1 succeeded.
03/26 15:17:50	vpn	informational	ipsec-key-install	pa-remote-101(pa-remote-101)	IPSec key installed. Installed SA: 203.0.113.8[500]-198.51.100.102[500] SPI:0x9AA85D81/0xDEB581DB lifetime 3600 Sec lifesize unlimited.
03/26 15:17:50	vpn	informational	ike-nego-p2-succ	pa-remote-101(pa-remote-101)	IKE phase-2 negotiation is succeeded as responder, quick mode. Established SA: 203.0.113.8[500]-198.51.100.102[500] message id:0x642CCD25, SPI:0x9AA85D81/0xDEB581DB.
03/26 15:17:50	vpn	informational	ike-nego-p2-start	198.51.100.102[500]	IKE phase-2 negotiation is started as responder, quick mode. Initiated SA: 203.0.113.8[500]-198.51.100.102[500] message id:0x642CCD25.
03/26 15:17:50	vpn	informational	ike-nego-p1-succ	pa-remote-101	IKE phase-1 negotiation is succeeded as responder, aggressive mode. Established SA: 203.0.113.8[500]-198.51.100.102[500] cookie:dd0c6a56020176ff:efd4bc2c7f100b44 lifetime 28800 Sec.
03/26 15:17:50	vpn	informational	ike-nego-p1-start	pa-remote-101	IKE phase-1 negotiation is started as responder, aggressive mode. Initiated SA: 203.0.113.8[500]-198.51.100.102[500] cookie:dd0c6a56020176ff:efd4bc2c7f100b44.

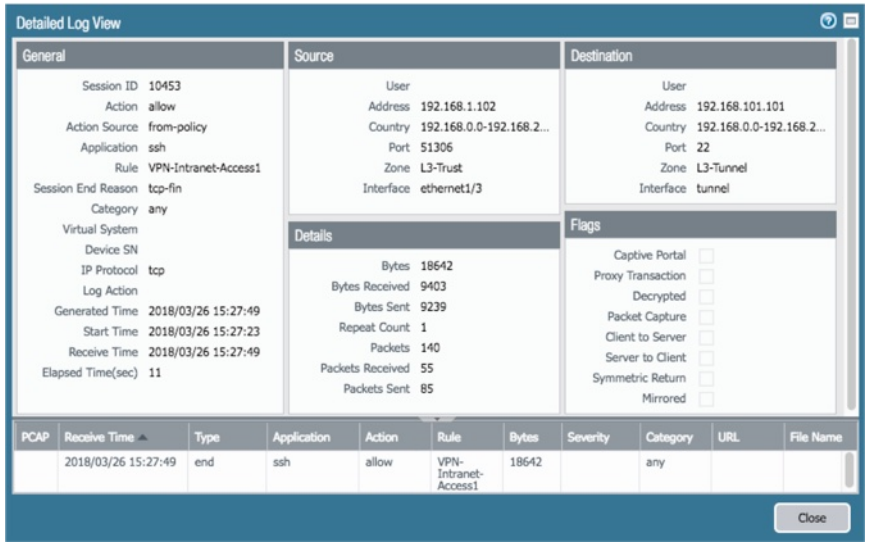
(subtype eq vpn)

表示フィルタを使用することで必要なログを素早く確認することが可能

センター側：設定後のトラフィックログ例

- センターサイトから拠点のサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

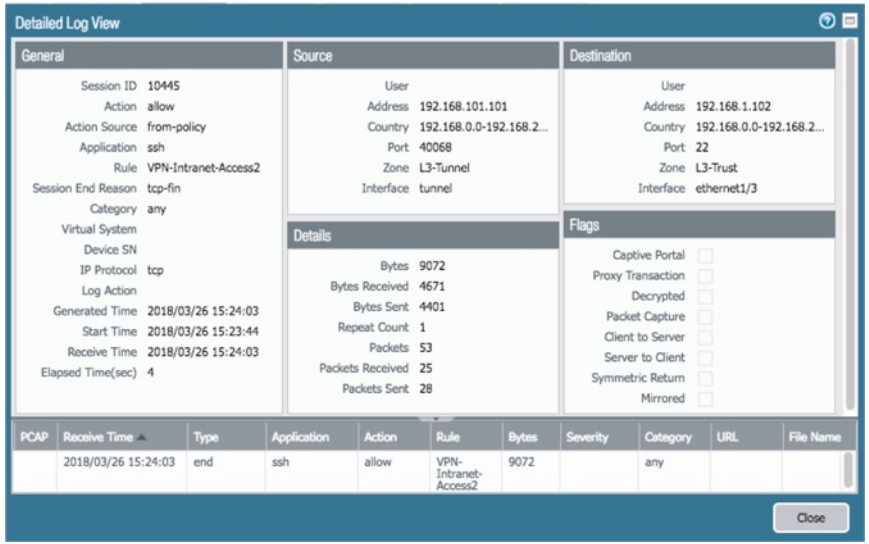
		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
		03/26 15:27:49	end	L3-Trust	L3-Tunnel	192.168.1.102		192.168.101.101	22	ssh	allow	VPN-Intranet-Access1	tcp-fin	18.6k



センター側：設定後のトラフィックログ例

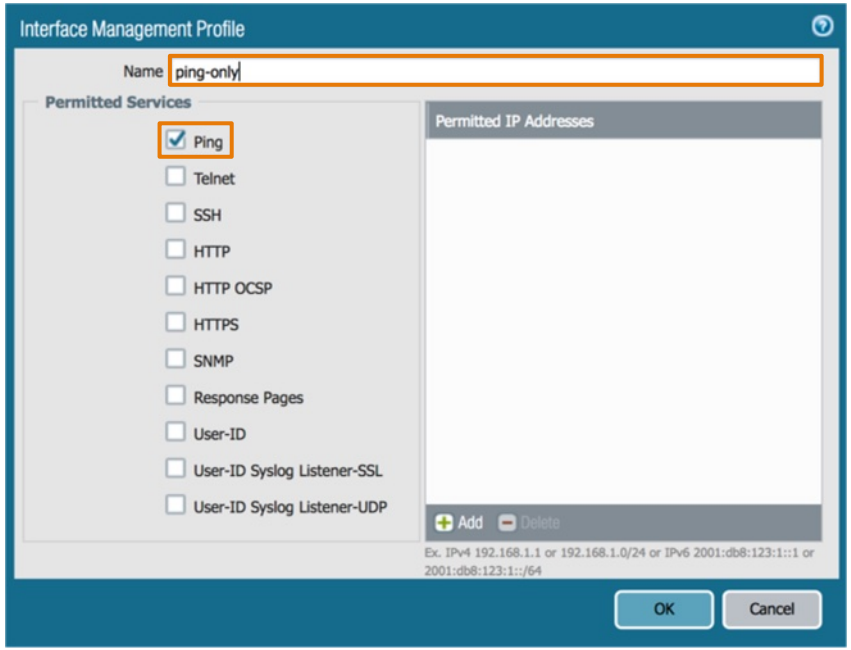
- 拠点からセンターサイトのサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
		03/26 15:24:03	end	L3-Tunnel	L3-Trust	192.168.101.101		192.168.1.102	22	ssh	allow	VPN-Intranet-Access2	tcp-fin	9.1k



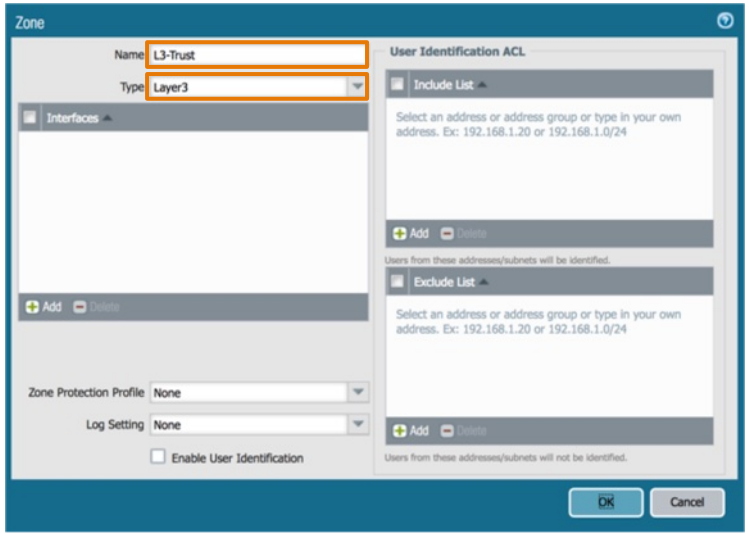
拠点側：インターフェイス管理アクセス設定

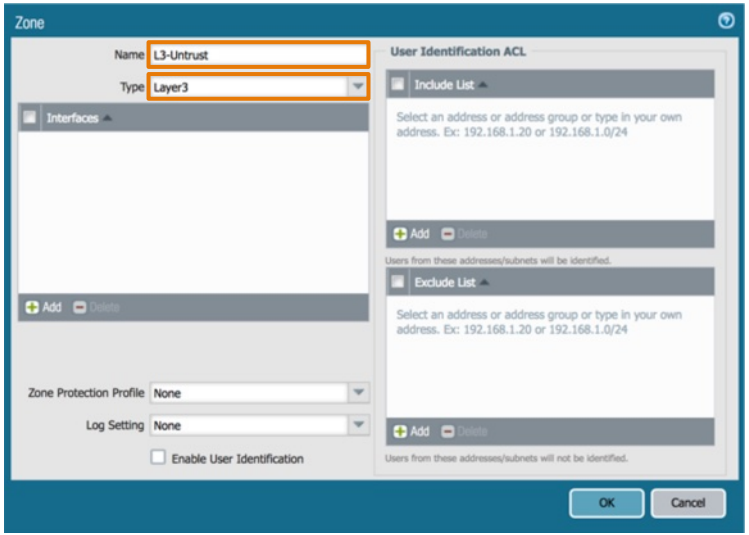
- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)



拠点側：セキュリティゾーン設定

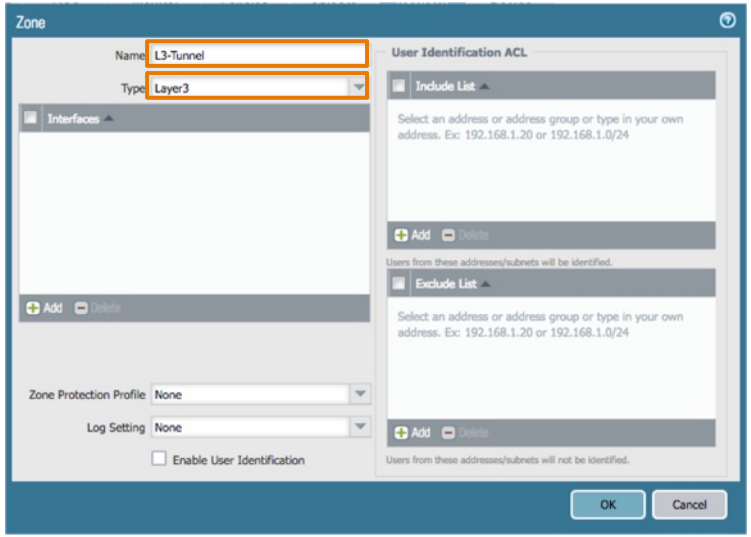
- 内部ネットワーク用、外部ネットワーク(インターネット)用セキュリティゾーンを作成(Network > Zones)





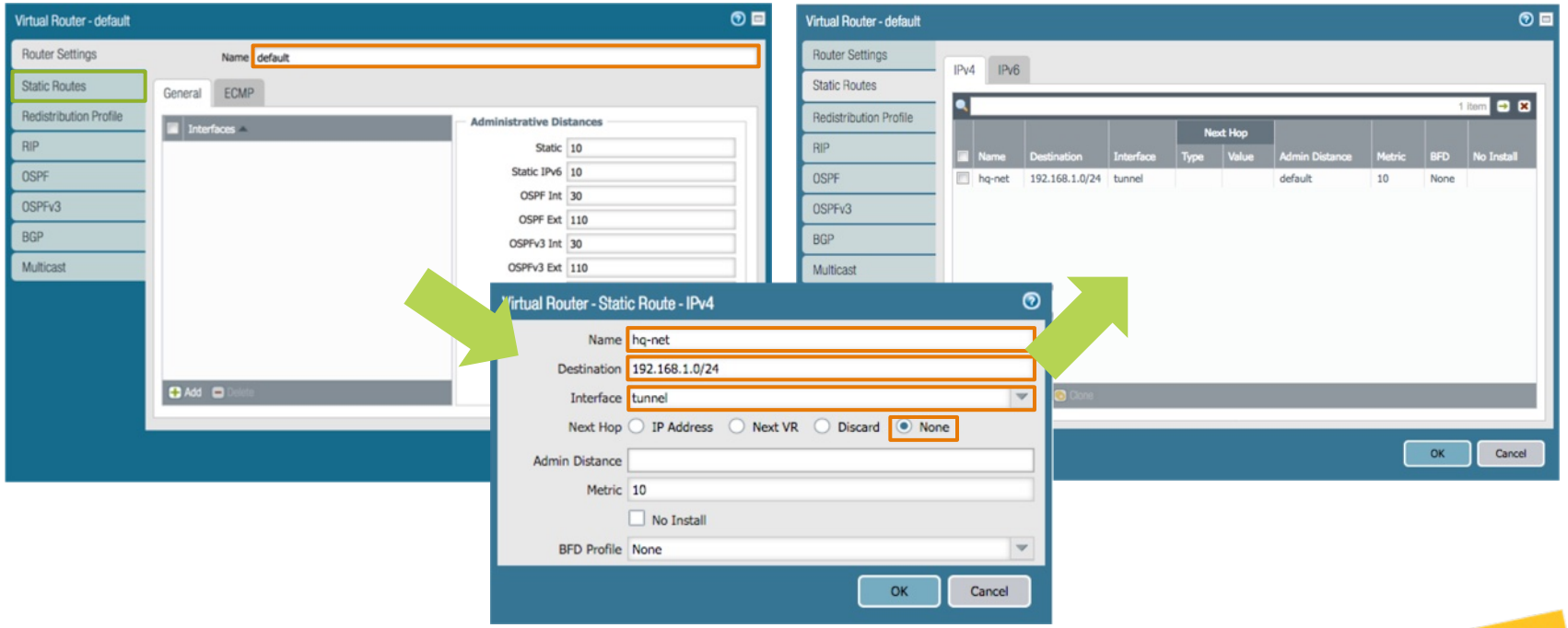
拠点側：セキュリティゾーン設定

- VPN通信用セキュリティゾーンを作成
(Network > Zones)



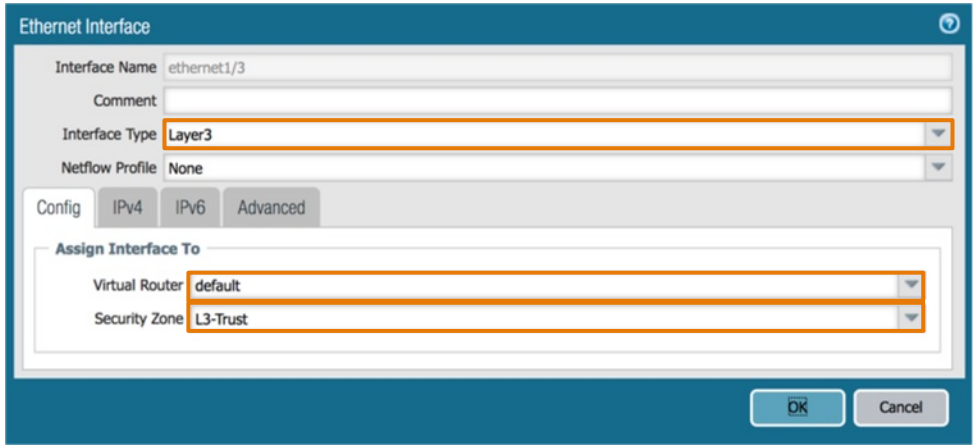
拠点側：仮想ルーター設定

- デフォルト仮想ルーター(default)に対して(VPN経由)本社内部ネットワーク向けStatic Routeを追加 (Network > Virtual Routers)



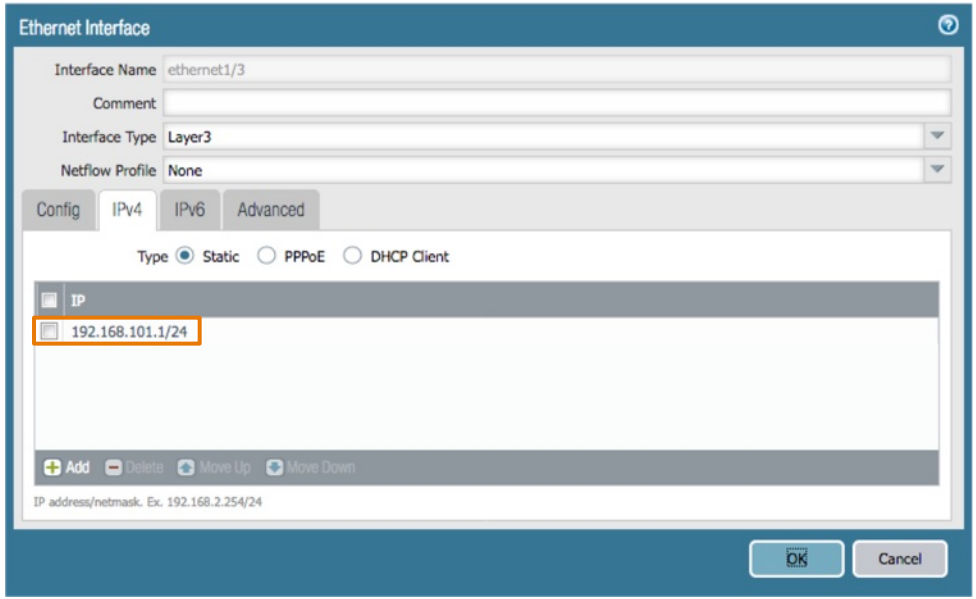
拠点側：内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



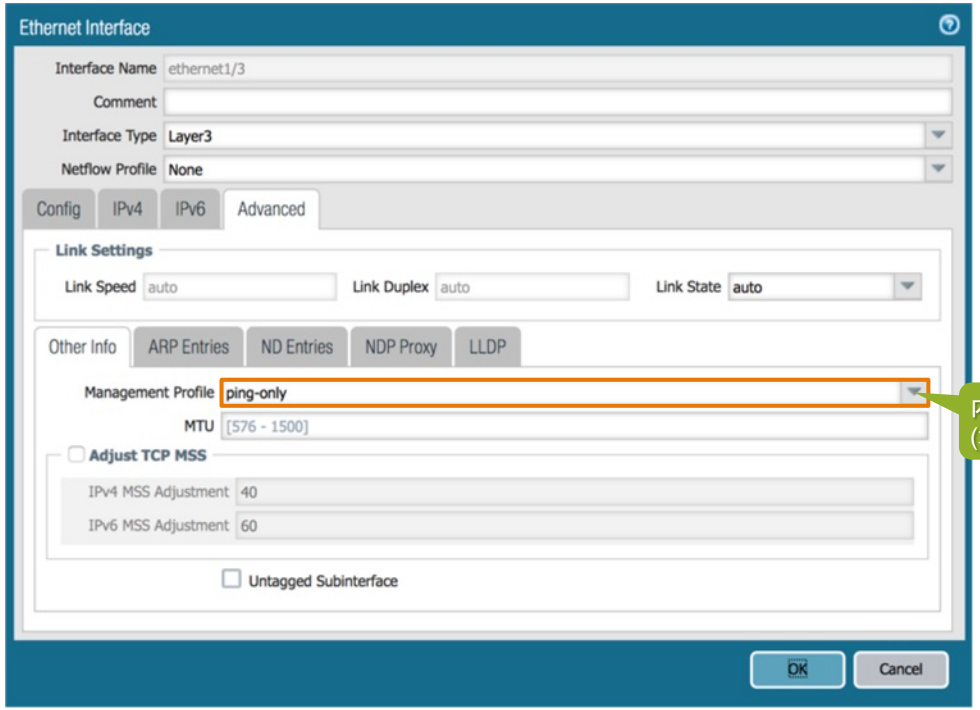
拠点側：内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



拠点側：内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



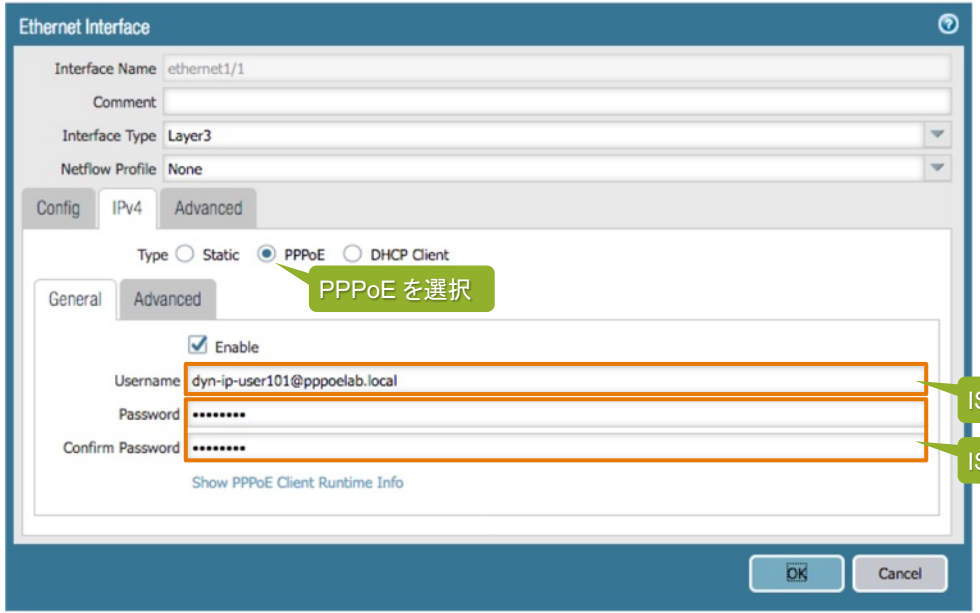
内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

拠点側：外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

拠点側：外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

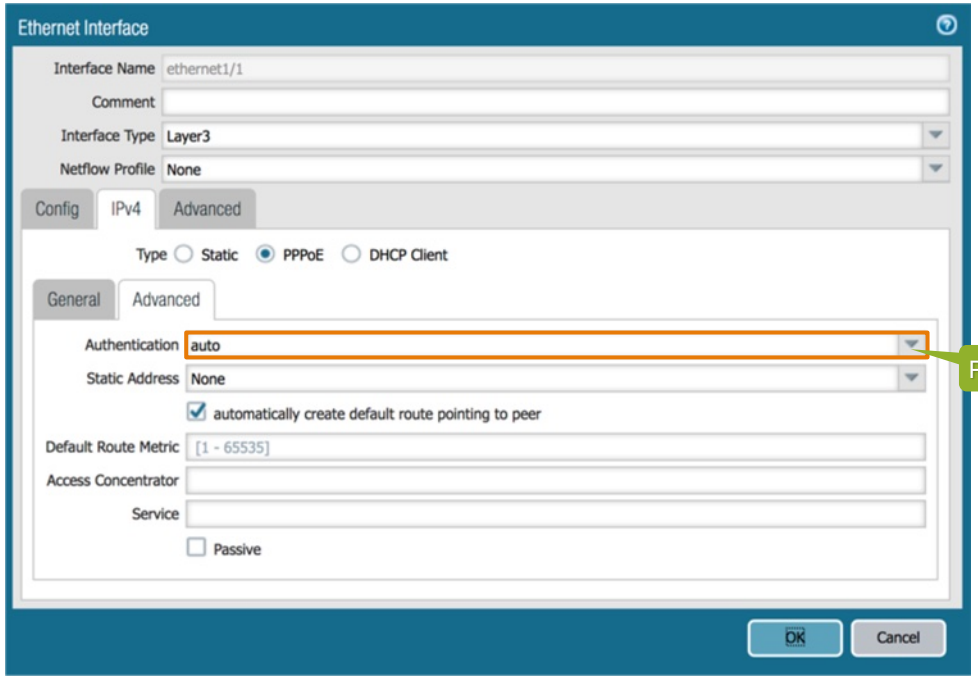


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

拠点側：外部ネットワーク用インターフェイス設定

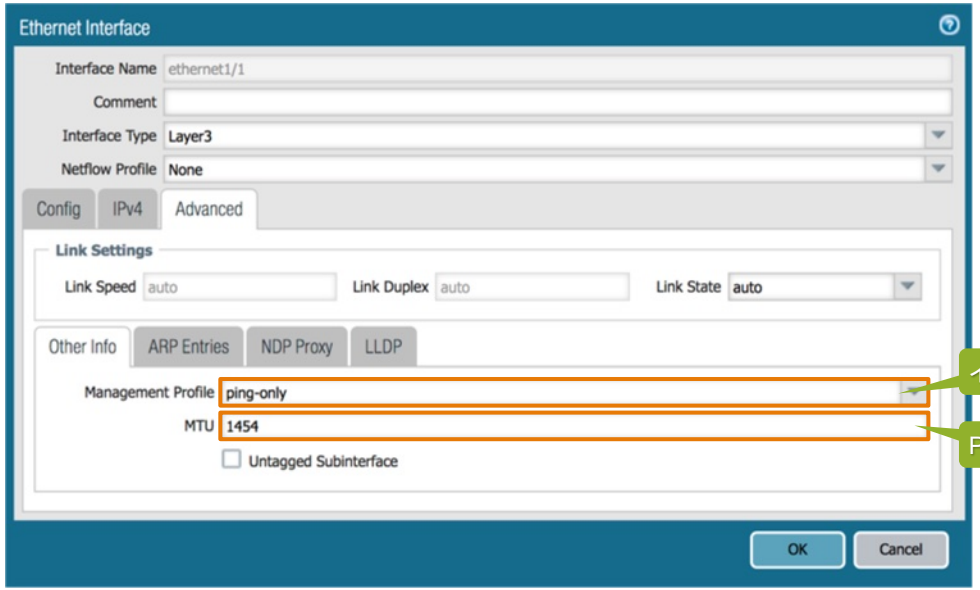
- ethernet1/1 インターフェイスの設定 (Network > Interfaces)



PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

拠点側：外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

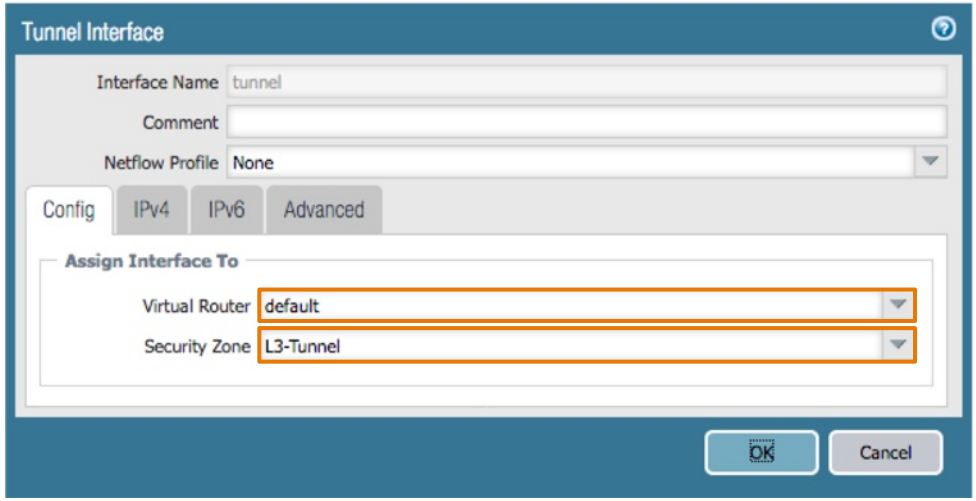


インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

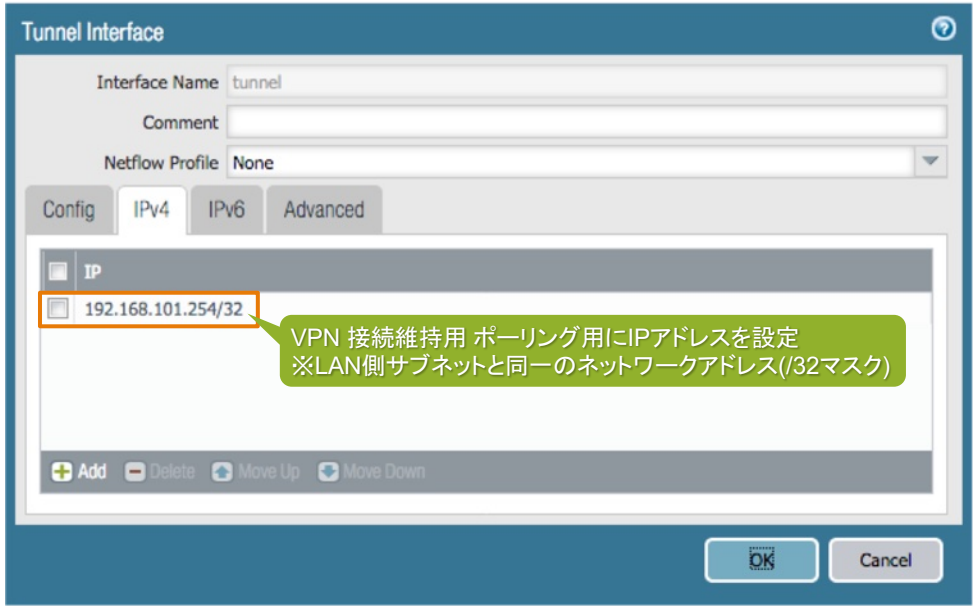
拠点側：VPN用論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



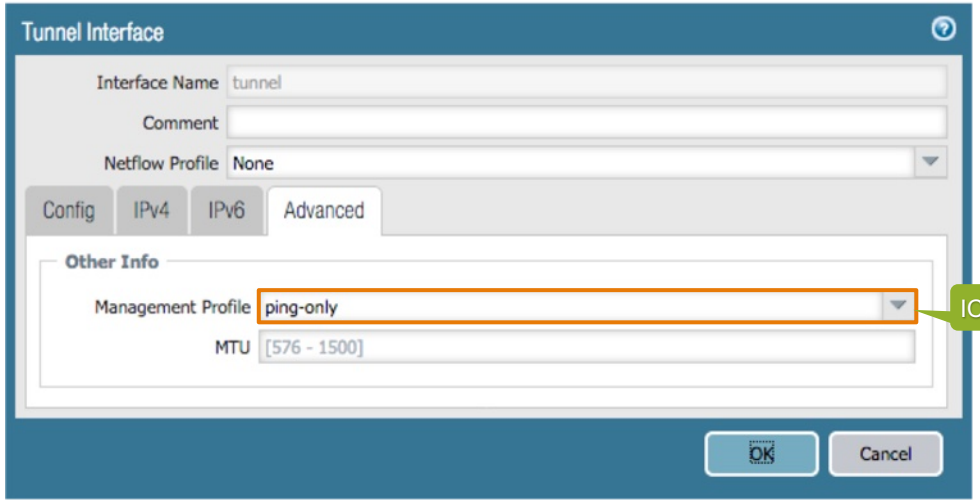
拠点側：VPN用論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



拠点側：VPN用論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



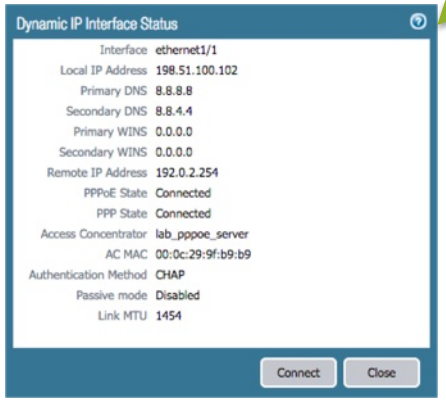
ICMP 疎通確認のための設定 (オプション)

拠点側：ネットワークインターフェイス設定一覧

- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

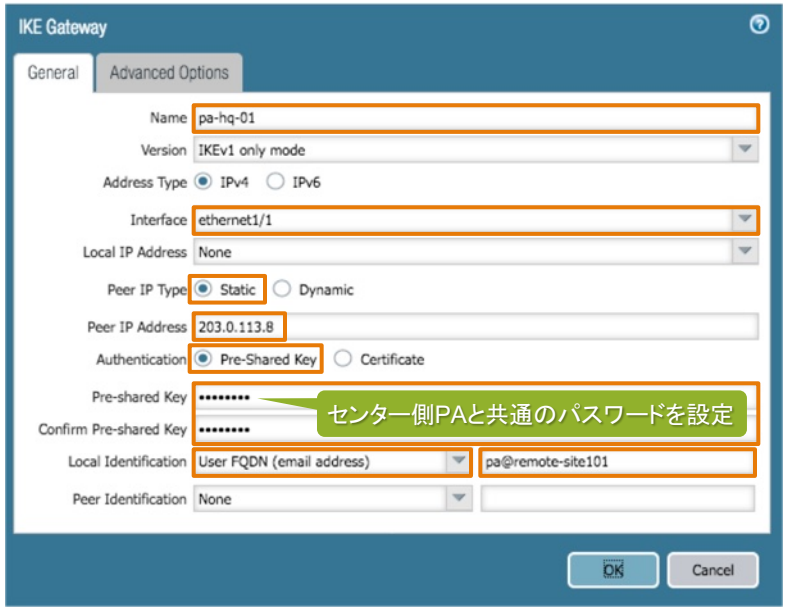
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone	Features
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	default	Untagged	L3-Untrust	
ethernet1/2				none	none	Untagged	none	
ethernet1/3	Layer3	ping-only		192.168.101.1/24	default	Untagged	L3-Trust	

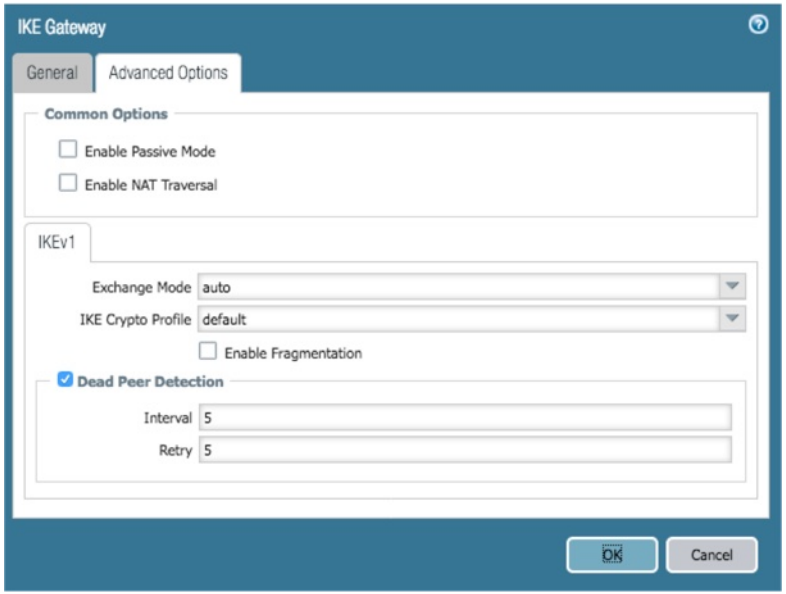
Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel	ping-only	192.168.101.254/32	default	L3-Tunnel		



拠点側：VPN接続用 IPSec IKE ゲートウェイ設定

- IKE Gateway (Network > Network Profiles > IKE Gateways)

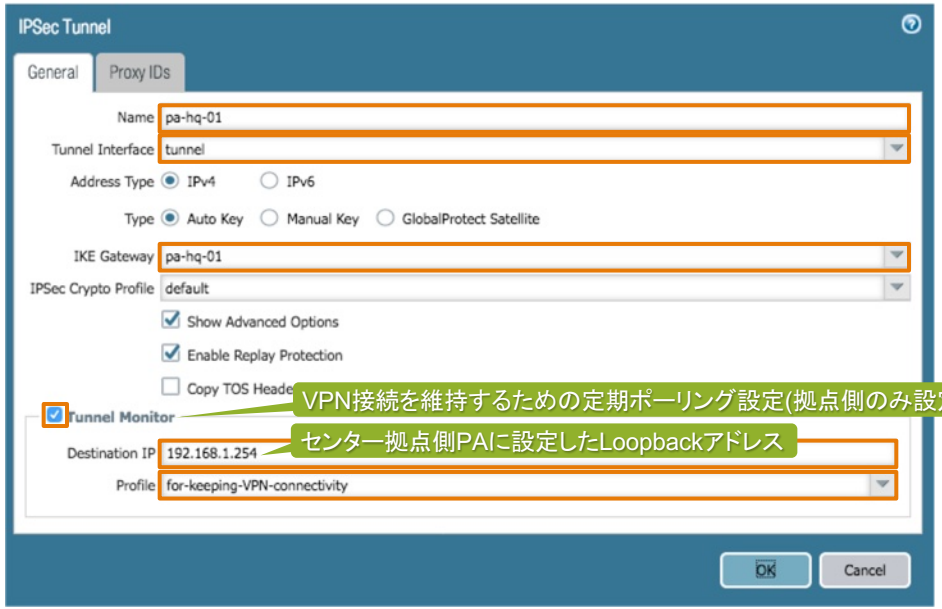




			Local Address		Peer ID		Local ID			IKE Advanced Options					
Name	Peer Address	Interface	IP	ID	Type	ID	Type	Version	Mode	Passive Mode	NAT Traversal	Crypto Profile	DPD	Liveness
pa-hq-01	203.0.113.8	ethernet1/1				pa@remote-site101	User FQDN (email address)	ikev1	auto			default	enabled/default/default	

拠点側：VPN接続用 IPSec トンネル設定

- IPSec Tunnel (Network > IPSec Tunnels)



VPN接続を維持するための定期ポーリング設定(拠点側のみ設定)

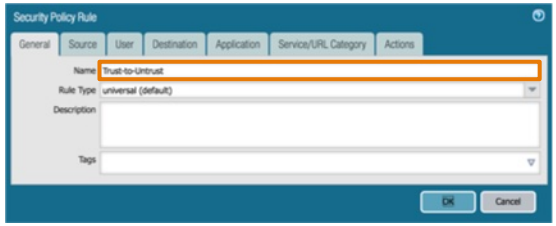
センター拠点側PAIに設定したLoopbackアドレス

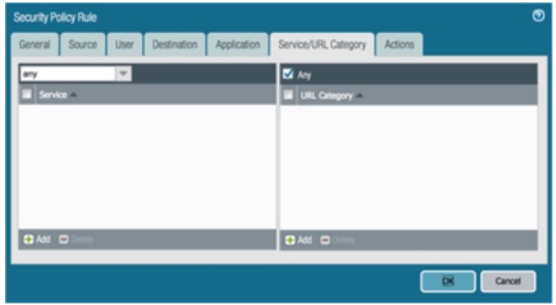
Network > Network Profiles > Monitor

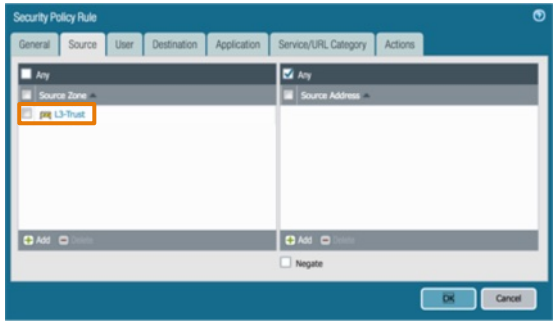
	Name	Status	Type	IKE Gateway/Satellite Interface	Local IP	Peer IP	Status	Tunnel Interface	Virtual Router	Virtual System	Security Zone	Status
	pa-hq-01	Tunnel Info	Auto Key	ethernet1/1		203.0.113.8	IKE Info	tunnel	default (Show Routes)	vsys1	L3-Tunnel	

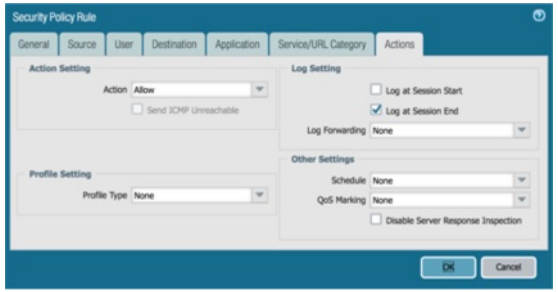
拠点側：セキュリティポリシー設定

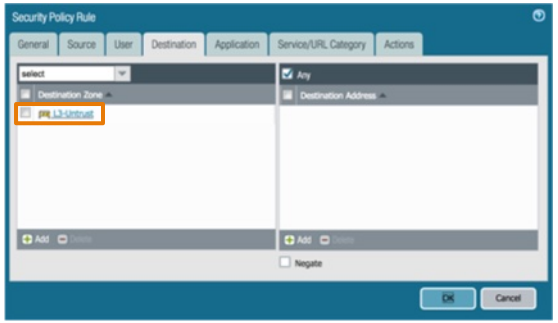
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)





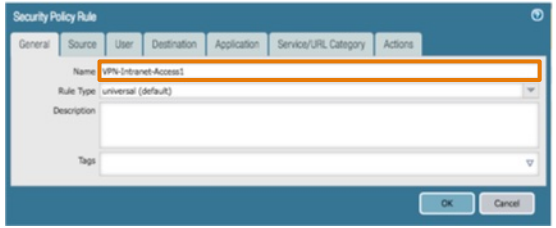


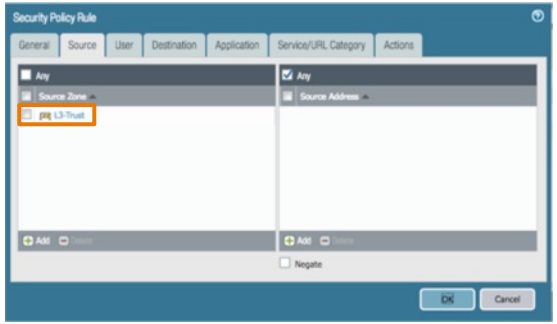


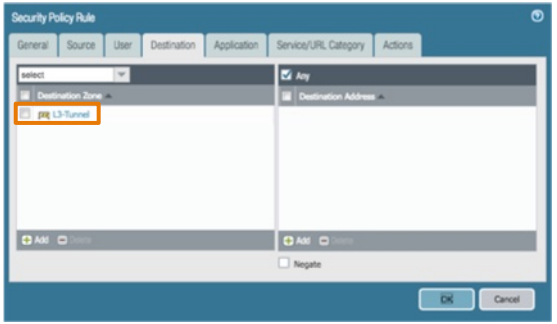


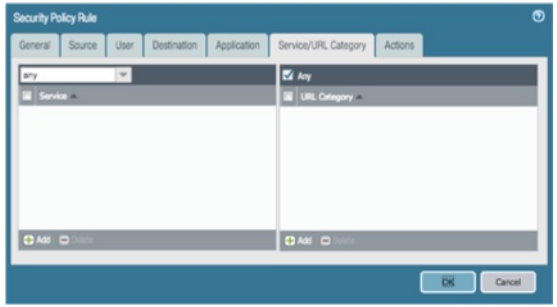
拠点側：セキュリティポリシー設定

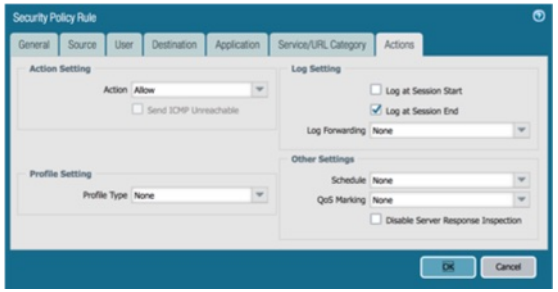
- センター拠点向けVPN通信用セキュリティポリシーの設定1 (Policies > Security)





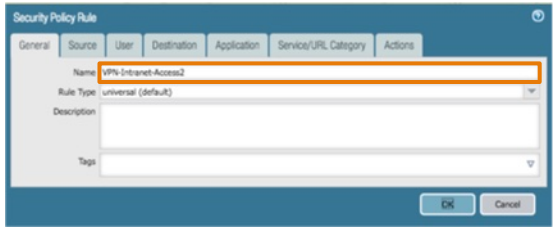


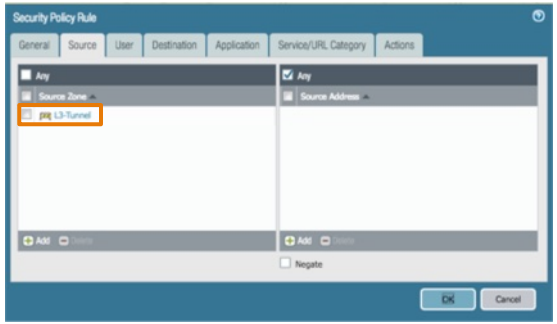


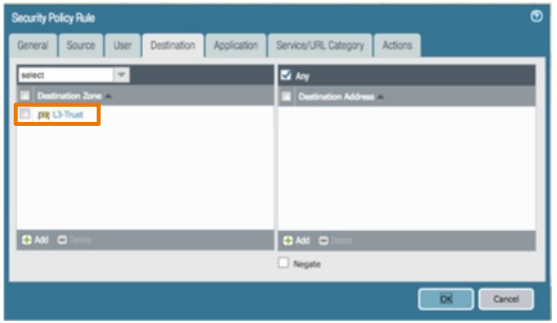


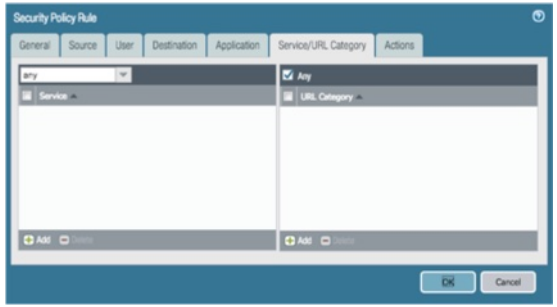
拠点側：セキュリティポリシー設定

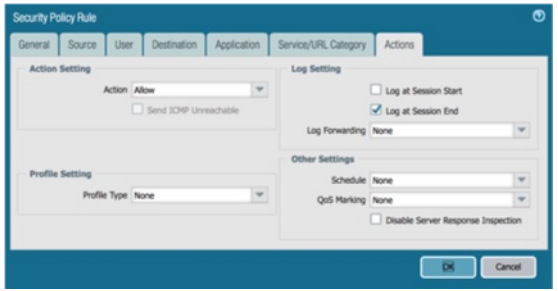
- センター拠点向けVPN通信用セキュリティポリシーの設定2 (Policies > Security)











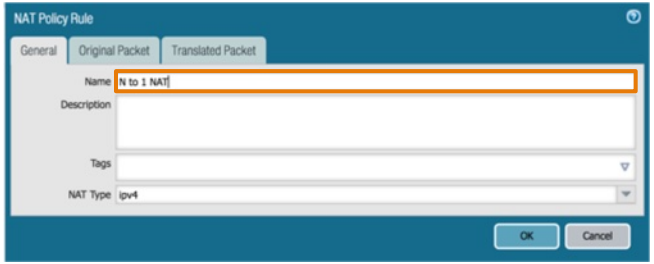
拠点側：セキュリティポリシー設定一覧

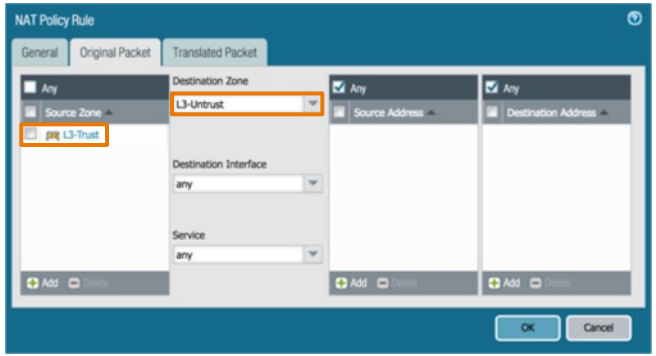
- セキュリティポリシー設定一覧 (Policies > Security)

				Source			Destination						
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
2	VPN-Intranet-Access1	none	universal	L3-Trust	any	any	L3-Tunnel	any	any	any	Allow	none	
3	VPN-Intranet-Access2	none	universal	L3-Tunnel	any	any	L3-Trust	any	any	any	Allow	none	
4	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

拠点側：NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)





IPアドレスは指定しなくて良い
(インターフェイス に割当てられた
IPアドレスが自動的に使われる)

拠点側：NATポリシー設定一覧

- NATポリシー設定一覧 (Policies > NAT)

	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

拠点側: 設定後のPPPoE 接続ログ

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/26 15:17:46	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:dyn-ip-user101@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:2, IP Address negotiated:198.51.100.102
03/26 15:17:42	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:dyn-ip-user101@pppoelab.local on interface:ethernet1/1

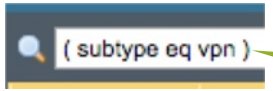
(subtype eq pppoe)

表示フィルタを使用することで必要なログを素早く確認することが可能

拠点側: 設定後のVPN 接続ログ

- VPN接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/26 15:17:50	vpn	informational	ipsec-key-install	pa-hq-01(pa-hq-01)	IPSec key installed. Installed SA: 198.51.100.102[500]-203.0.113.8[500] SPI:0xDEB581DB/0x9AA85D81 lifetime 3600 Sec lifesize unlimited.
03/26 15:17:50	vpn	informational	ike-nego-p2-succ	pa-hq-01(pa-hq-01)	IKE phase-2 negotiation is succeeded as initiator, quick mode. Established SA: 198.51.100.102[500]-203.0.113.8[500] message id:0x642CCD25, SPI:0xDEB581DB/0x9AA85D81.
03/26 15:17:50	vpn	informational	ike-nego-p2-start	pa-hq-01(pa-hq-01)	IKE phase-2 negotiation is started as initiator, quick mode. Initiated SA: 198.51.100.102[500]-203.0.113.8[500] message id:0x642CCD25.
03/26 15:17:50	vpn	informational	ike-nego-p1-succ	pa-hq-01	IKE phase-1 negotiation is succeeded as initiator, aggressive mode. Established SA: 198.51.100.102[500]-203.0.113.8[500] cookie:dd0c6a56020176ff:efd4bc2c7f100b44 lifetime 28800 Sec.
03/26 15:17:50	vpn	informational	ike-nego-p1-start	pa-hq-01	IKE phase-1 negotiation is started as initiator, aggressive mode. Initiated SA: 198.51.100.102[500]-203.0.113.8[500] cookie:dd0c6a56020176ff:0000000000000000.

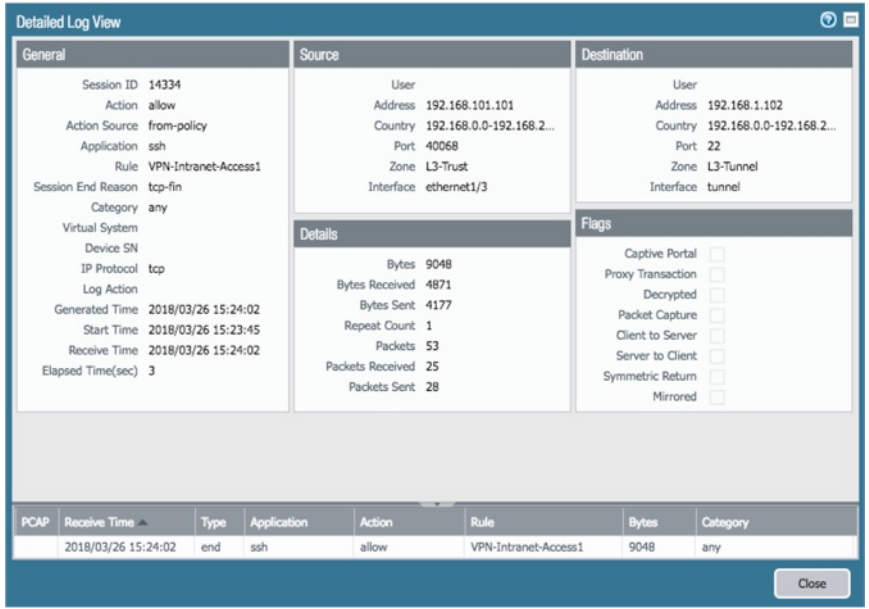


表示フィルタを使用することで必要なログを素早く確認することが可能

拠点側：設定後のトラフィックログ例

- 拠点からセンターサイトのサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

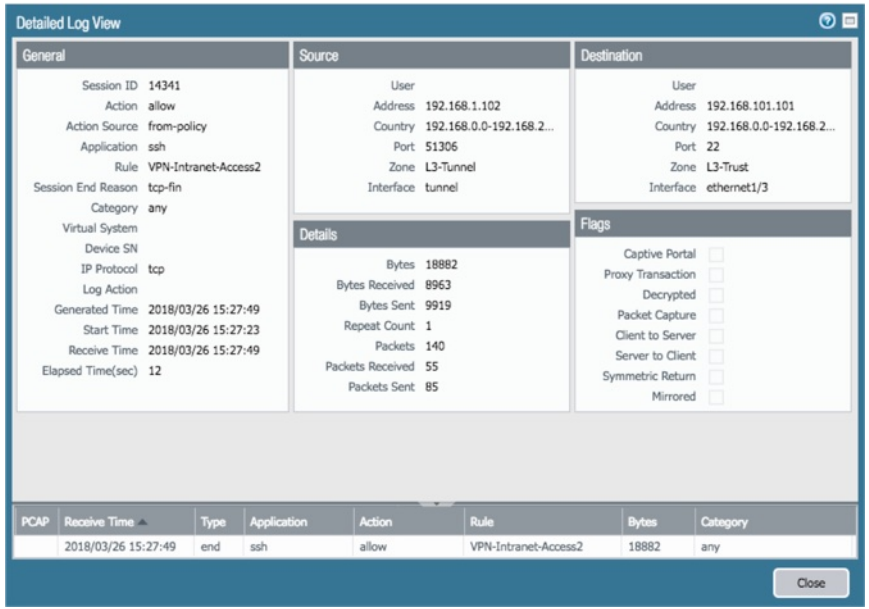
		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 15:24:02	end	L3-Trust	L3-Tunnel	192.168.101.101	192.168.1.102	22	ssh	any	allow	VPN-Intranet-Access1	tcp-fin	9.0k



拠点側：設定後のトラフィックログ例

- センターサイトから拠点のサーバへ通信した場合のログ例 (Monitor > Logs > Traffic)

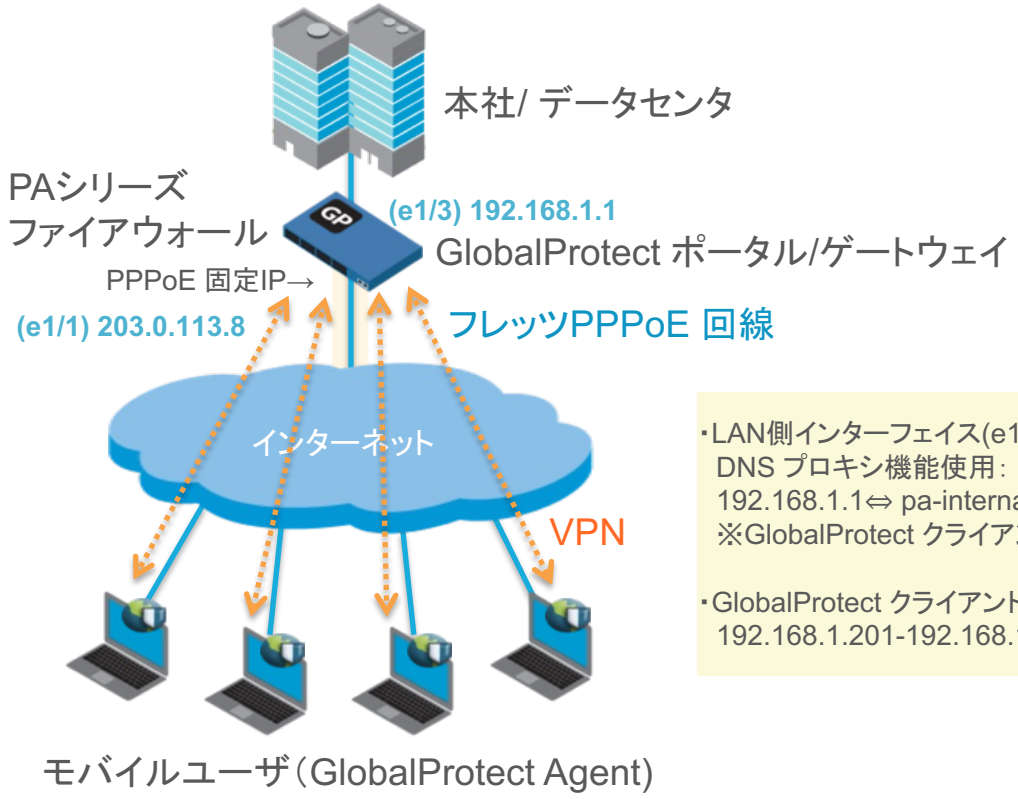
		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/26 15:27:49	end	L3-Tunnel	L3-Trust	192.168.1.102	192.168.101.101	22	ssh	any	allow	VPN-Intranet-Access2	tcp-fin	18.9k



PPPoE 設定例５

PPPoE 回線を使用したインターネット接続と
GlobalProtect クライアント接続

システム構成：



・LAN側インターフェイス(e1/3 192.168.1.1)において
DNS プロキシ機能使用：
192.168.1.1⇔ pa-internal-ip.pppoelab.local
※GlobalProtect クライアント 接続先ネットワーク自動判別用

・GlobalProtect クライアントに割り当てるIPアドレス範囲：
192.168.1.201-192.168.1.210

コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE 関連	・MTU 値を必ず変更する。（例：1454） ・PPPoE 認証方式はデフォルトのままで問題なし。 ・GlobalProtect ポータル/ゲートウェイ機能を使用する PPPoE インターフェイスには必ず明示的にIPアドレスを設定して下さい。
その他	・本番環境において使用する CA証明書、PAのGlobalProtect ポータル/ゲートウェイ用サーバ証明書は、組織で利用している証明書サービスなどで発行されたものをご利用下さい。 ・本番環境では GlobalProtect クライアント証明書を使用し、接続クライアントの正当性チェックを行う様にして下さい。 ・本番環境ではローカルユーザDBではなくActiveDirectoryやLDAPなどユーザ認証基盤によるユーザ認証を行う様構成して下さい。

☆実環境においては、各種脅威防御やURLフィルタリング WildFireなど、重要なセキュリティ機能を必ず設定・ご利用下さい。

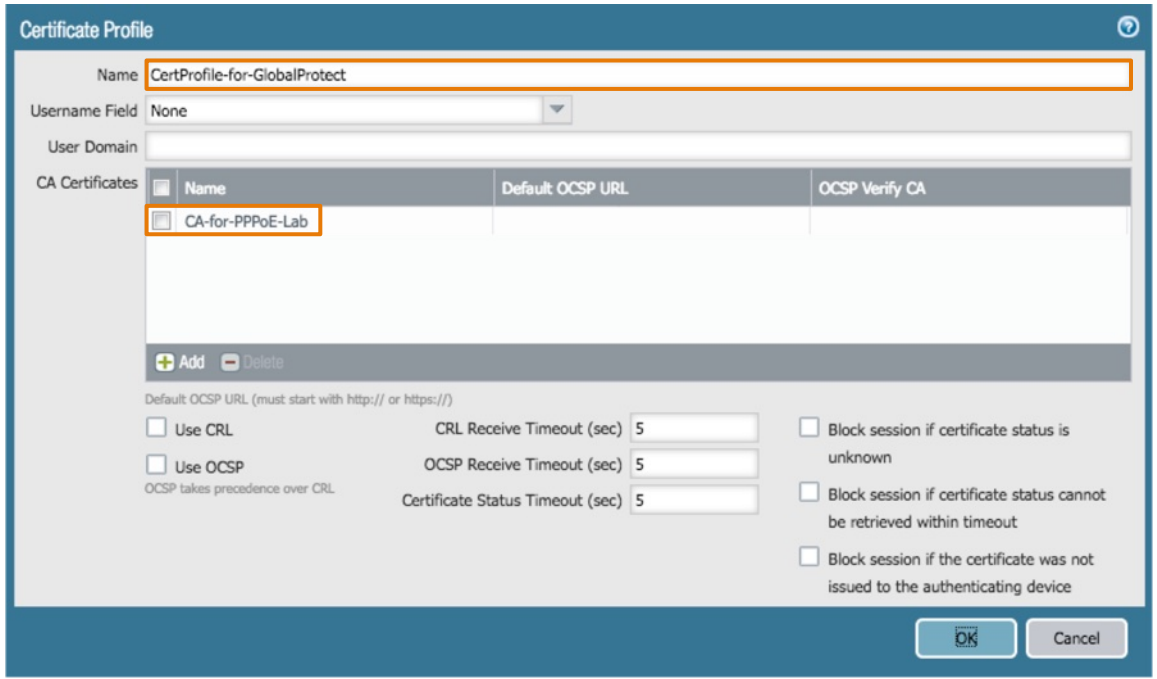
GlobalProtect用 証明書の生成

- CA証明書, Portal, 外部ゲートウェイ,内部ゲートウェイ用サーバ証明書を生成
(Device > Certificate Management > Certificates > Generate)

Name	Subject	Issuer	CA	Key	Expires	Status	Algorit...	Usage
CA-for-PPPoE-Lab	CN = CA-for-PPPoE-Lab	CN = CA-for-PPPoE-Lab	☑	☑	Mar 26 08:05:19 2019 GMT	valid	RSA	Trusted Root CA Certificate
Cert-for-GP-Ext-GW-and-Portal	CN = 203.0.113.8	CN = CA-for-PPPoE-Lab	☐	☑	Mar 26 08:09:12 2019 GMT	valid	RSA	
Cert-for-GP-Int-GW	CN = 192.168.1.1	CN = CA-for-PPPoE-Lab	☐	☑	Mar 26 23:38:09 2019 GMT	valid	RSA	

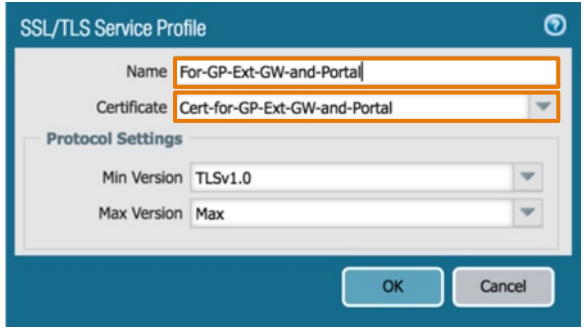
GlobalProtect用 証明書プロファイルの生成

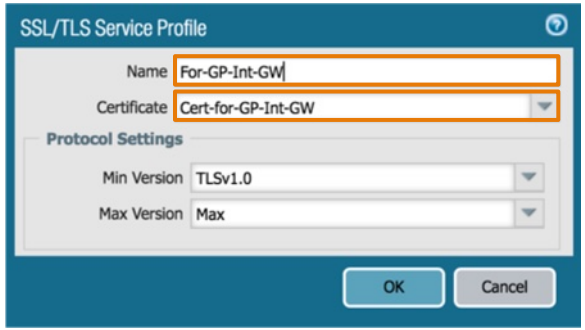
- 証明書プロファイルの作成
(Device > Certificate Management > Certificate Profile > Add)



GlobalProtect用 SSL/TLSサービスプロファイルの生成

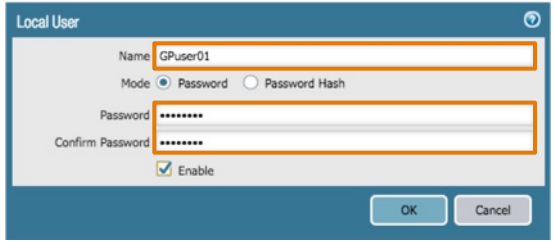
- GP Portal, 外部GW, 内部GWへのSSL接続時のサーバ証明書との紐付け設定
(Device > Certificate Management > SSL/TLS Service Profile > Add)

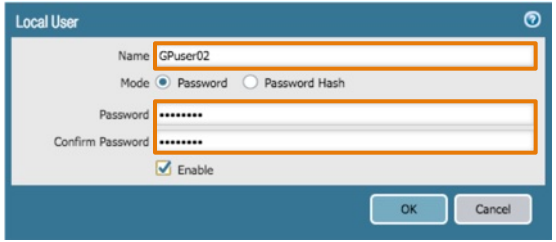


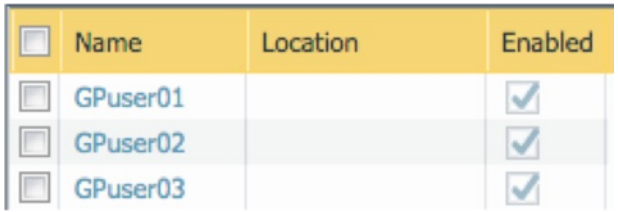


GlobalProtect ユーザ認証用ローカルユーザの作成

- ローカルユーザの作成
  (Device > local User Database > Users > Add)

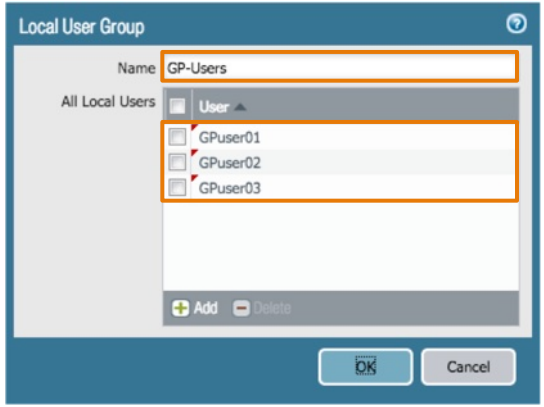






GlobalProtect ユーザ認証用ローカルグループの作成

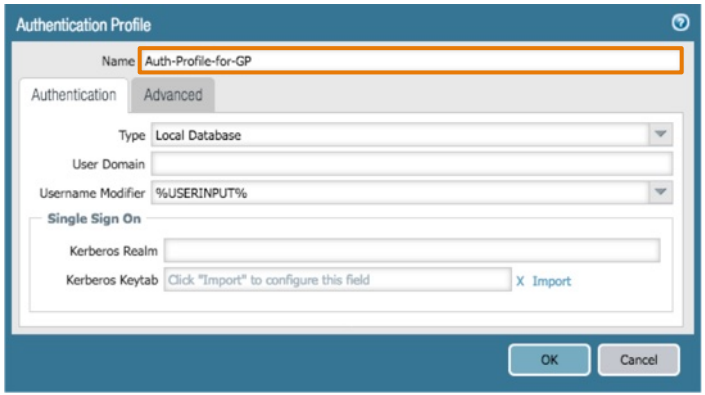
- ローカルユーザグループの作成
  (Device > local User Database > User Groups > Add)

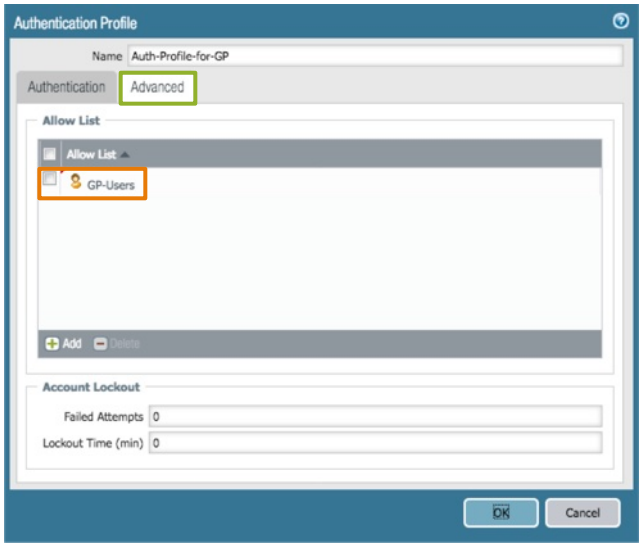


Name	Location	Local Users
GP-Users		GPuser01
		GPuser02
		GPuser03

GlobalProtect ユーザ認証用 認証プロファイルの作成

- GlobalProtect ユーザ認証用プロファイルの作成
  (Device > Authentication Profile > Add)

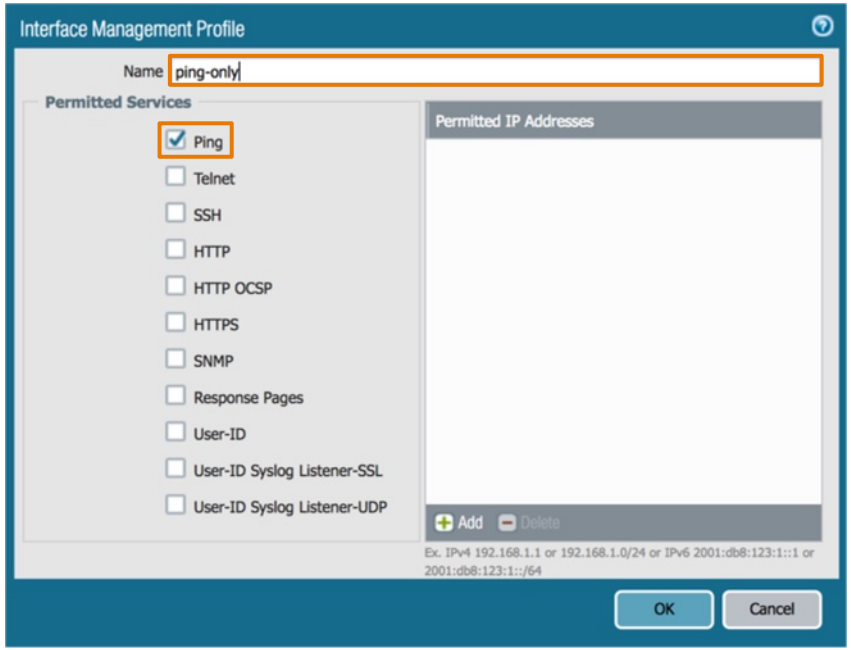




	Name	Location	Lockout		Allow List	Authentication	Server Profile	Others	Locked Users
			Failed Attempts (#)	Lockout Time (min)					
	Auth-Profile-for-GP		0 (default)	0 (default)	GP-Users	Local			none

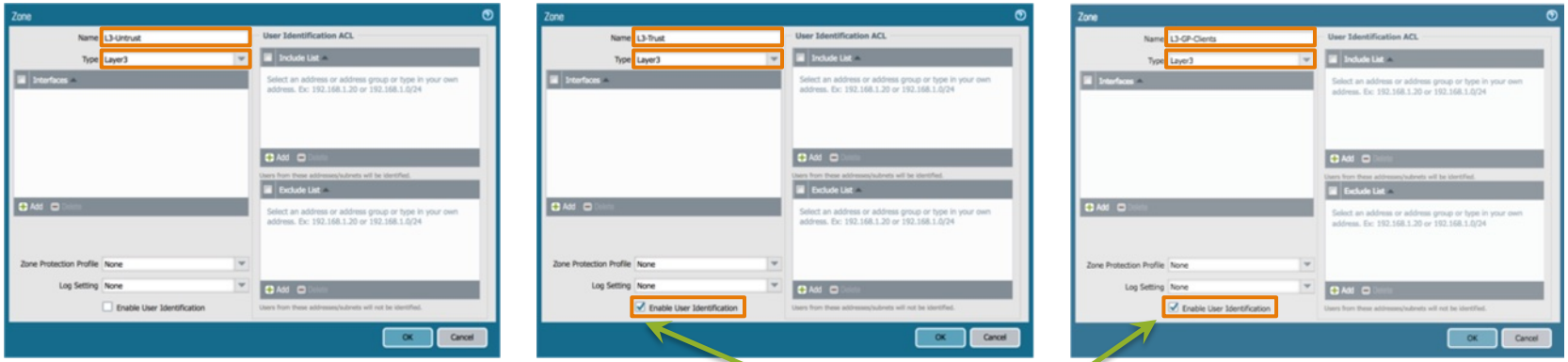
インターフェイス管理アクセス設定

- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)



セキュリティゾーン設定

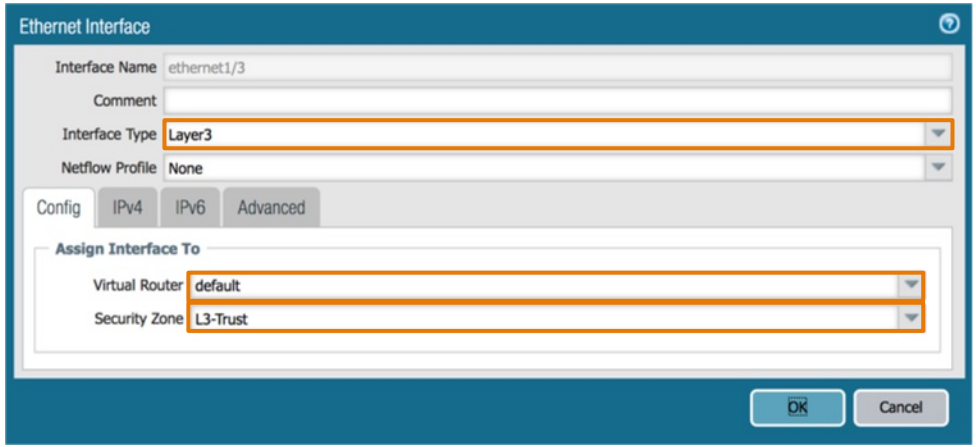
- 外部ネットワーク, 内部ネットワーク, GPクライアント用セキュリティゾーンを作成 (Network > Zones)



GlobalProtect ユーザに対するユーザ識別 (User-ID) 処理を有効にするためにチェック

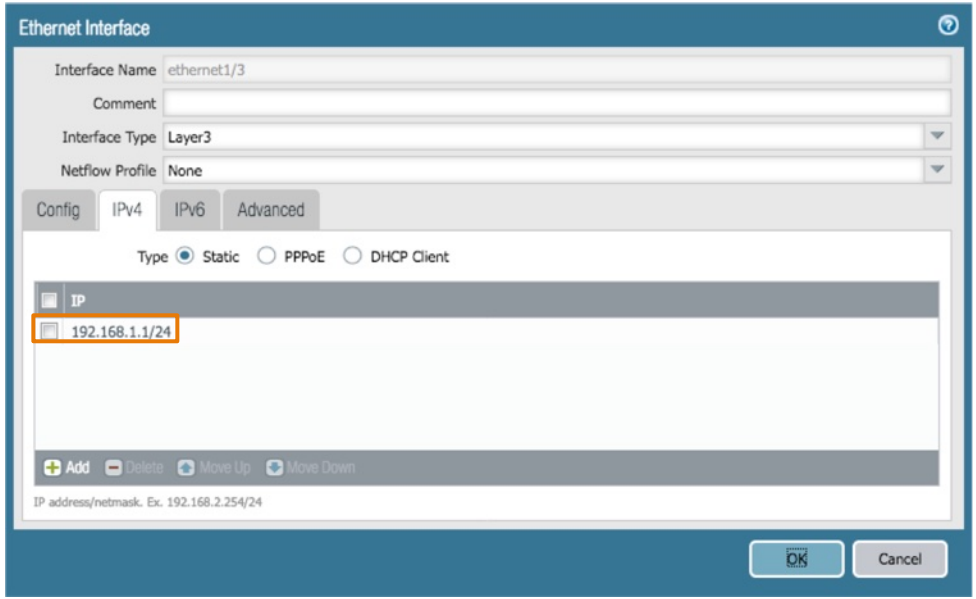
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



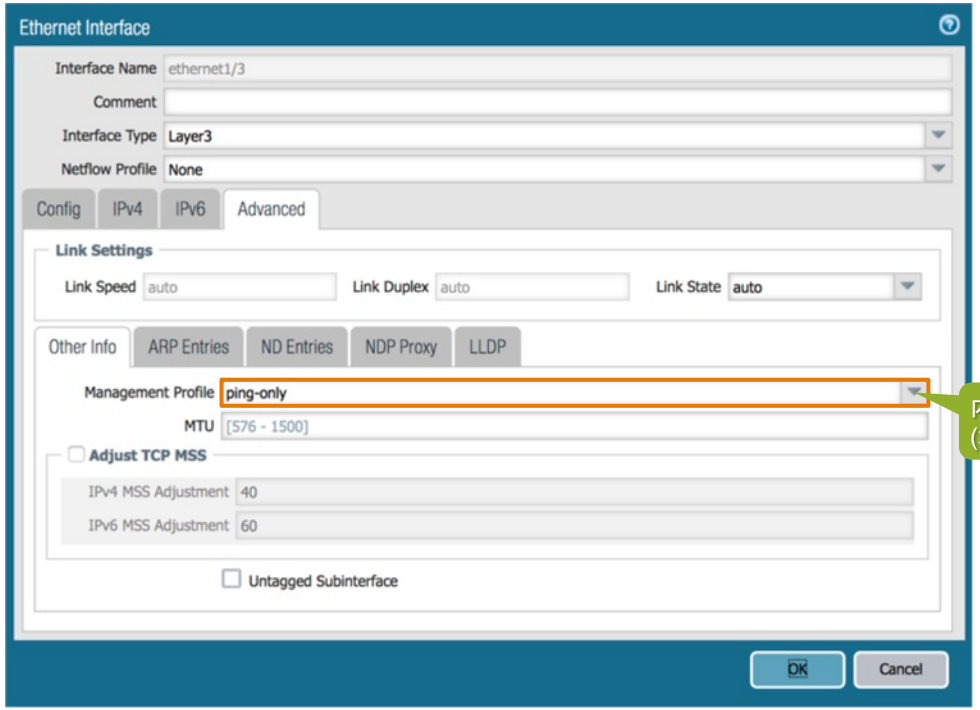
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



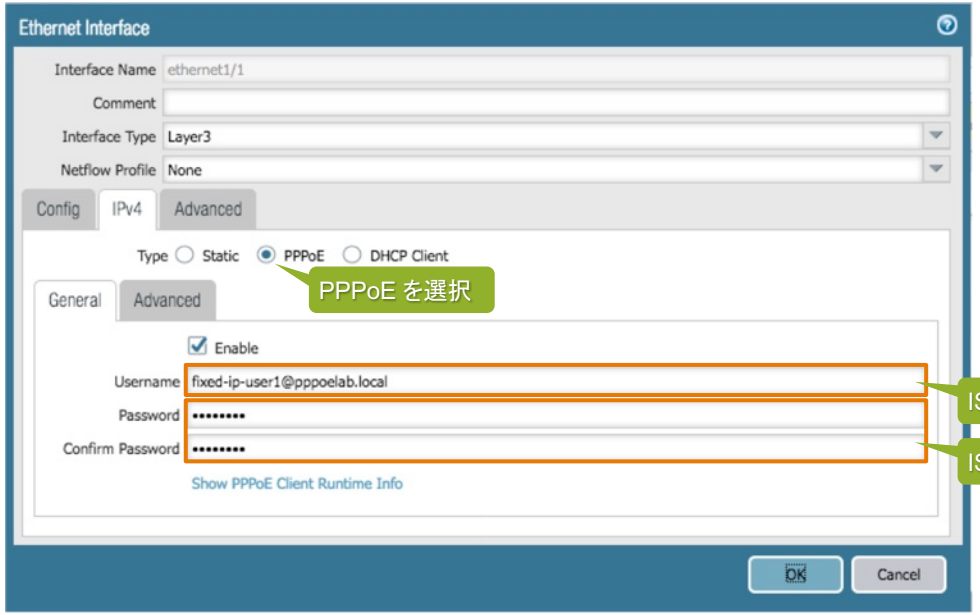
内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

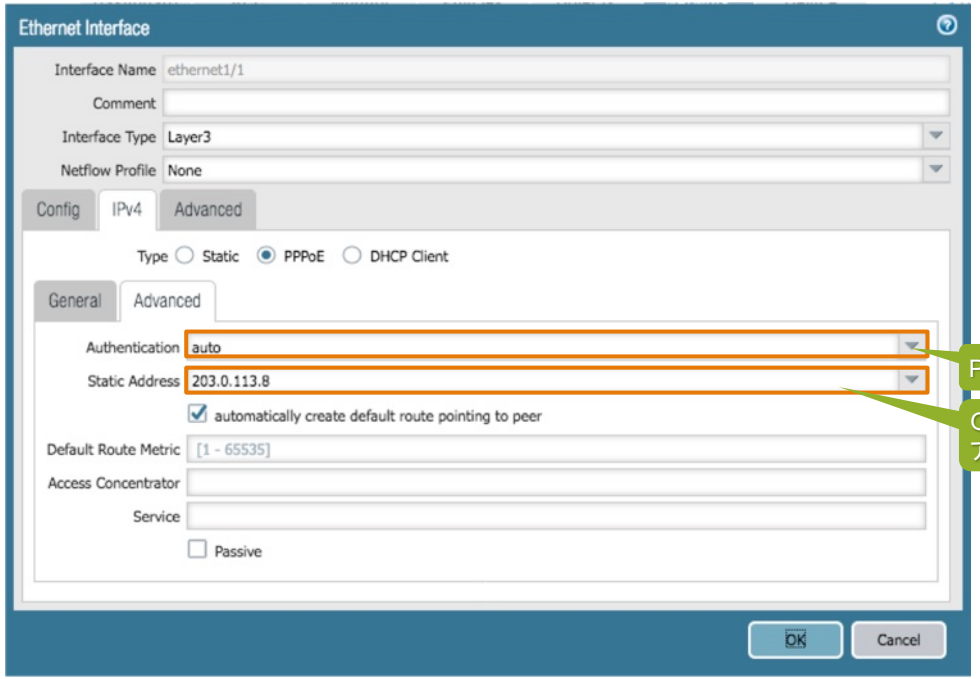


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

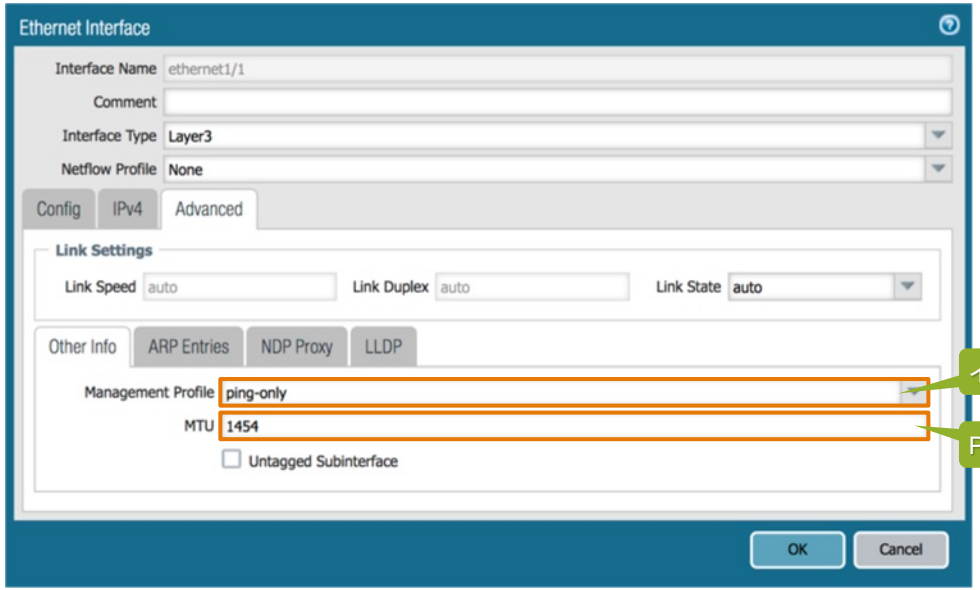


PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

GlobalProtect Portal/External Gateway 用として使用する IP アドレス(ISPがPPPoE I/Fに割り当てるアドレス) を設定

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

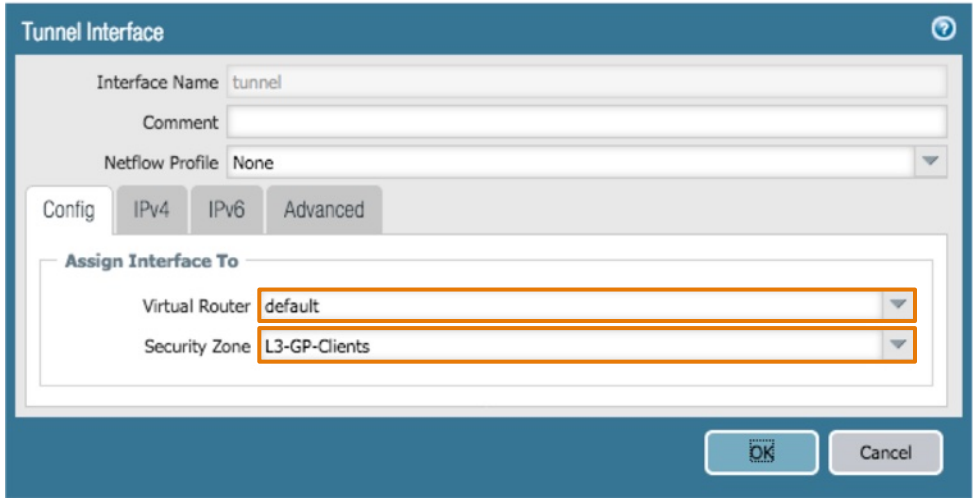


インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

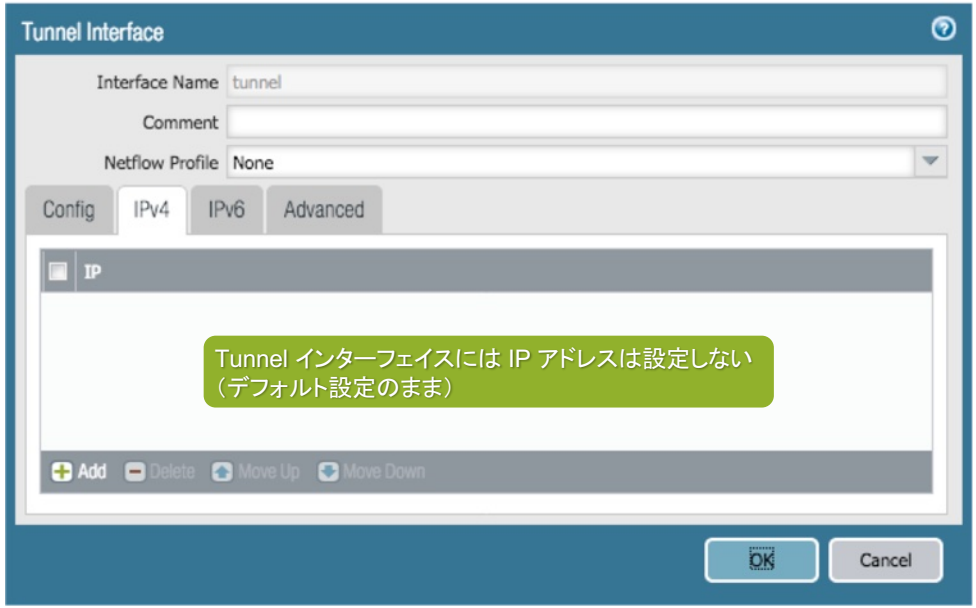
GlobalProtect VPN 終端用 論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



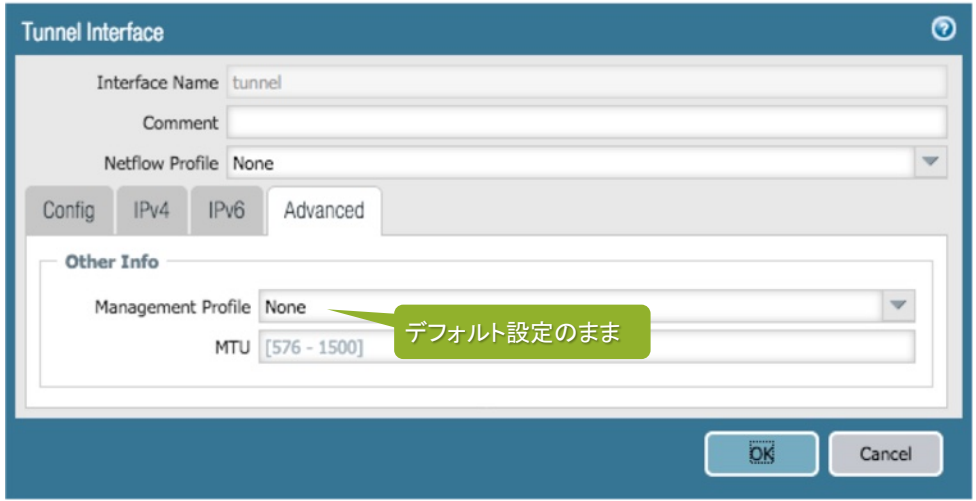
GlobalProtect VPN 終端用 論理インターフェイス設定

- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



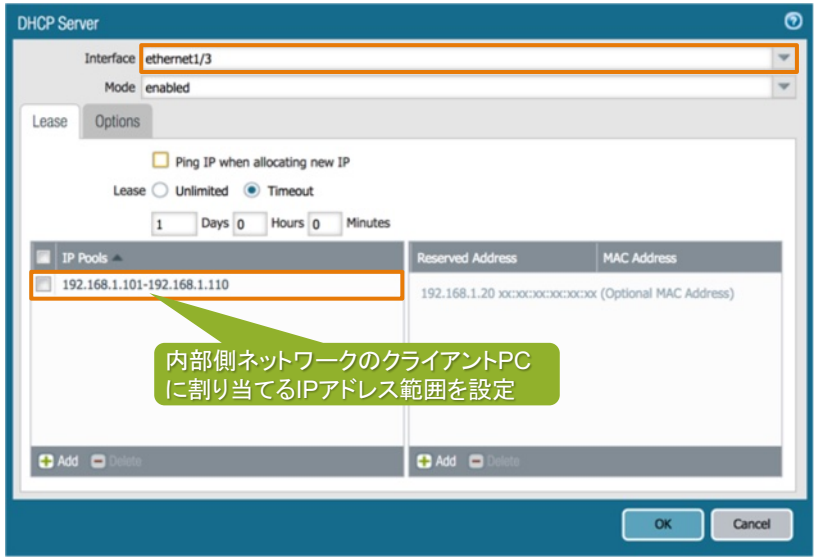
GlobalProtect VPN 終端用 論理インターフェイス設定

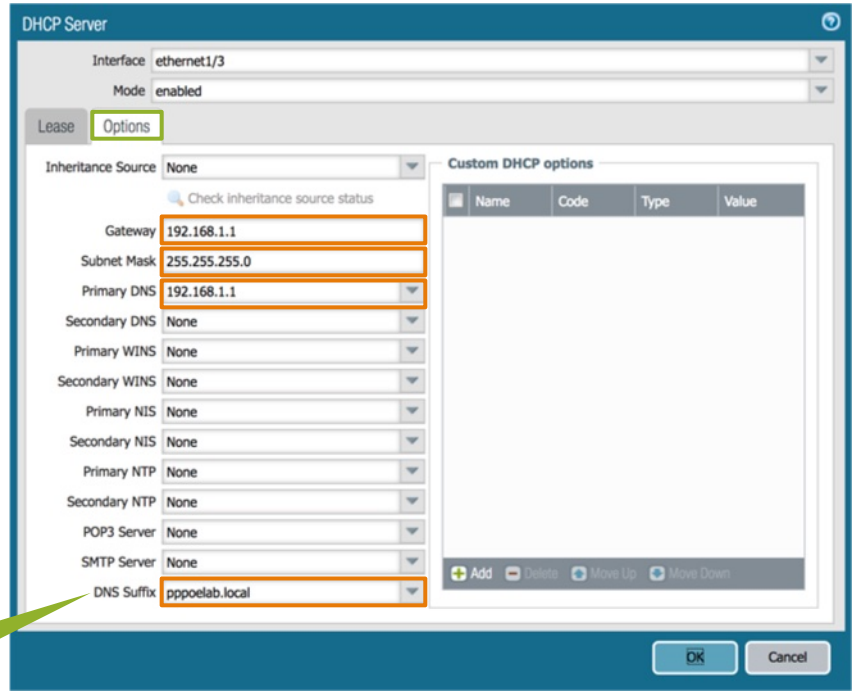
- tunnel インターフェイスの設定 (Network > Interfaces > Tunnel)



内部ネットワーク用 **DHCP**サーバ 設定

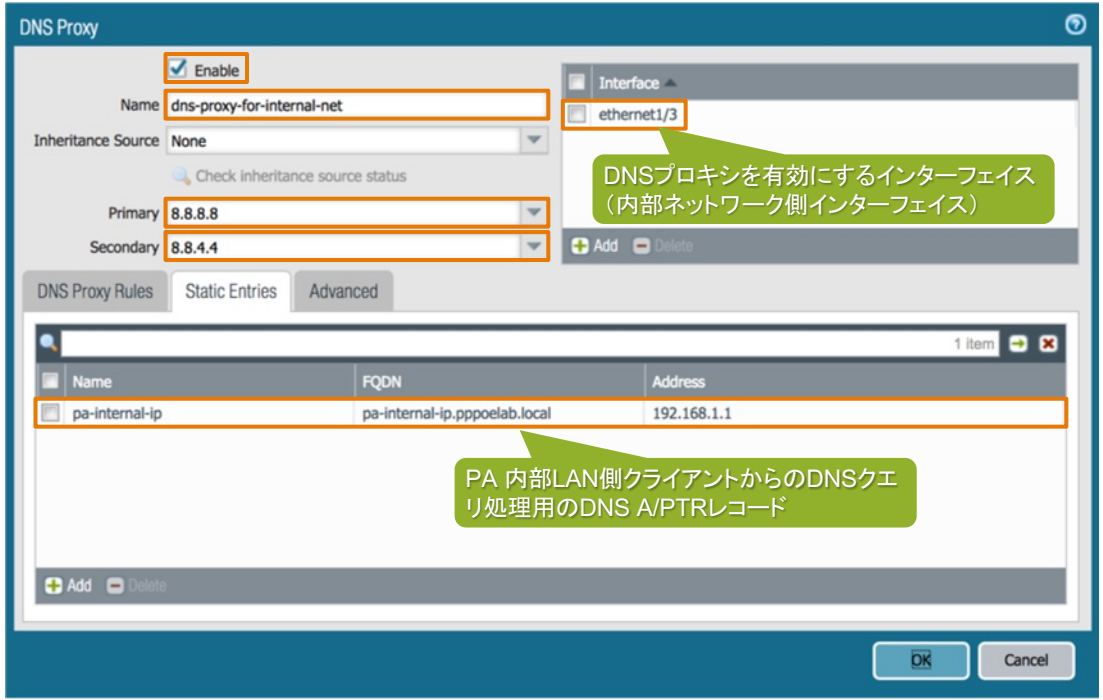
- DHCPサーバ の設定 (Network > DHCP > DHCP Server > Add)





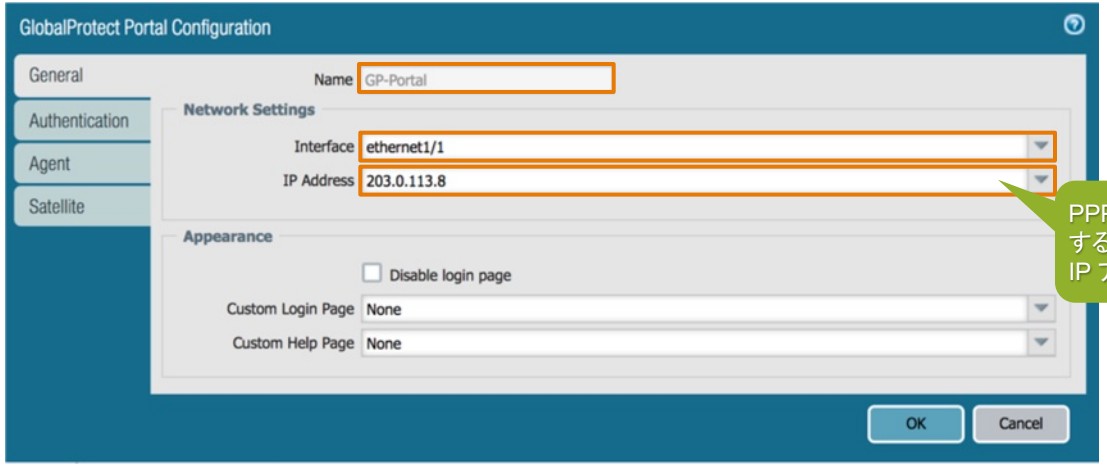
GlobalProtect DNS Reverse Lookup用 DNS Proxy 設定

- DNS Proxy の設定 (Network > DNS Proxy > Add)



GlobalProtect ポータル 設定

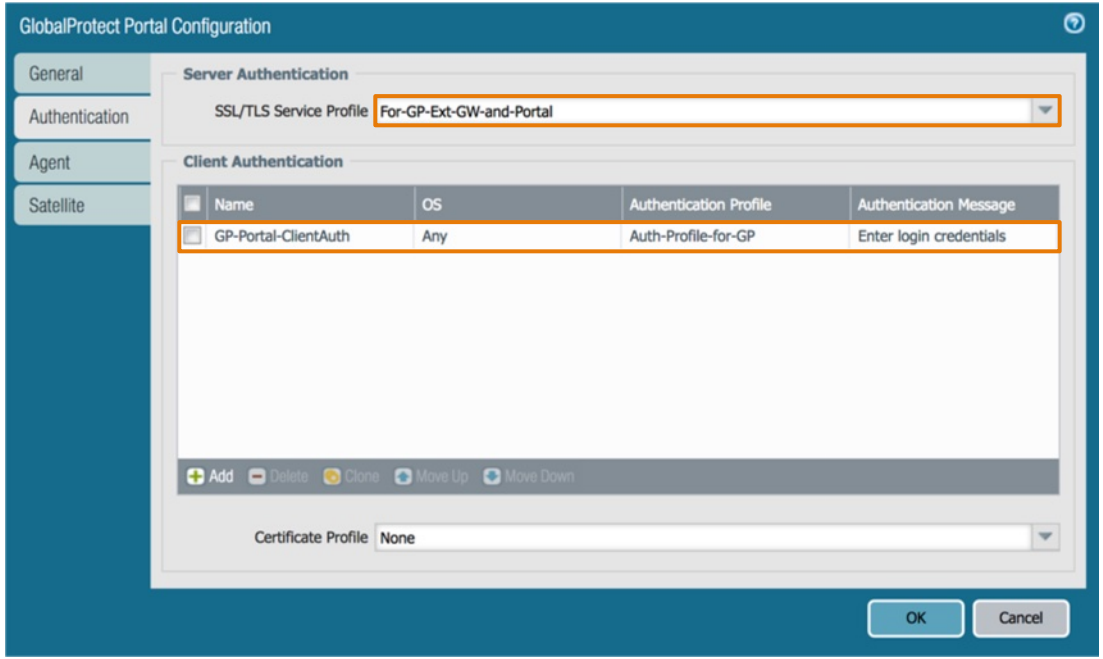
- GP ポータルの設定 (Network > GlobalProtect > Portals > Add)



PPPoEを使用するLAN IFにIPアドレスを設定することで、GlobalProtect ポータルで使用するIP アドレスの指定が出来る様になる

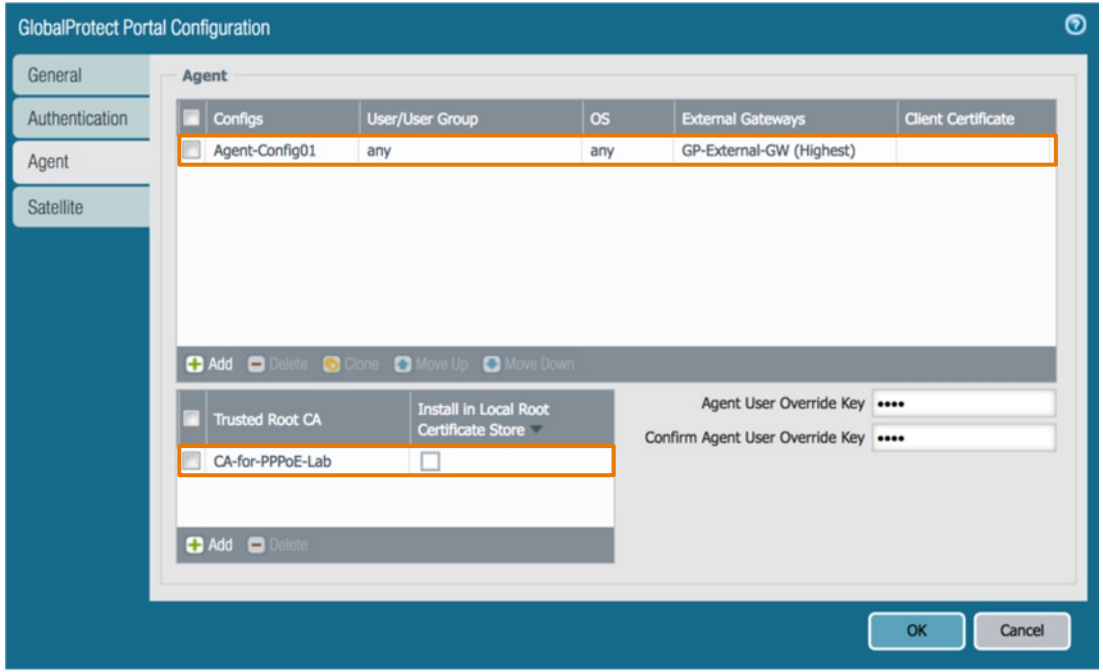
GlobalProtect ポータル 設定

- GP ポータルの設定 (Network > GlobalProtect > Portals)



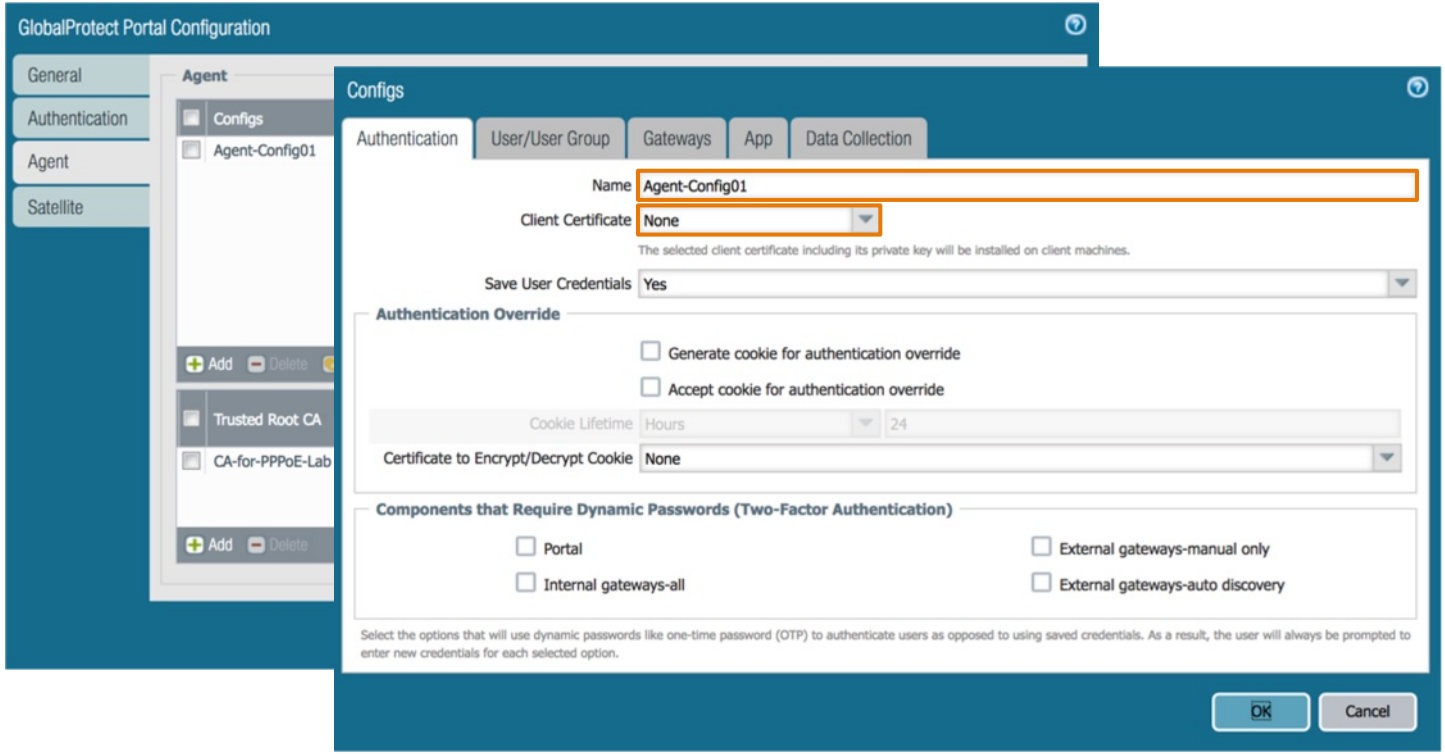
GlobalProtect ポータル 設定

- GP ポータルの設定 (Network > GlobalProtect > Portals)



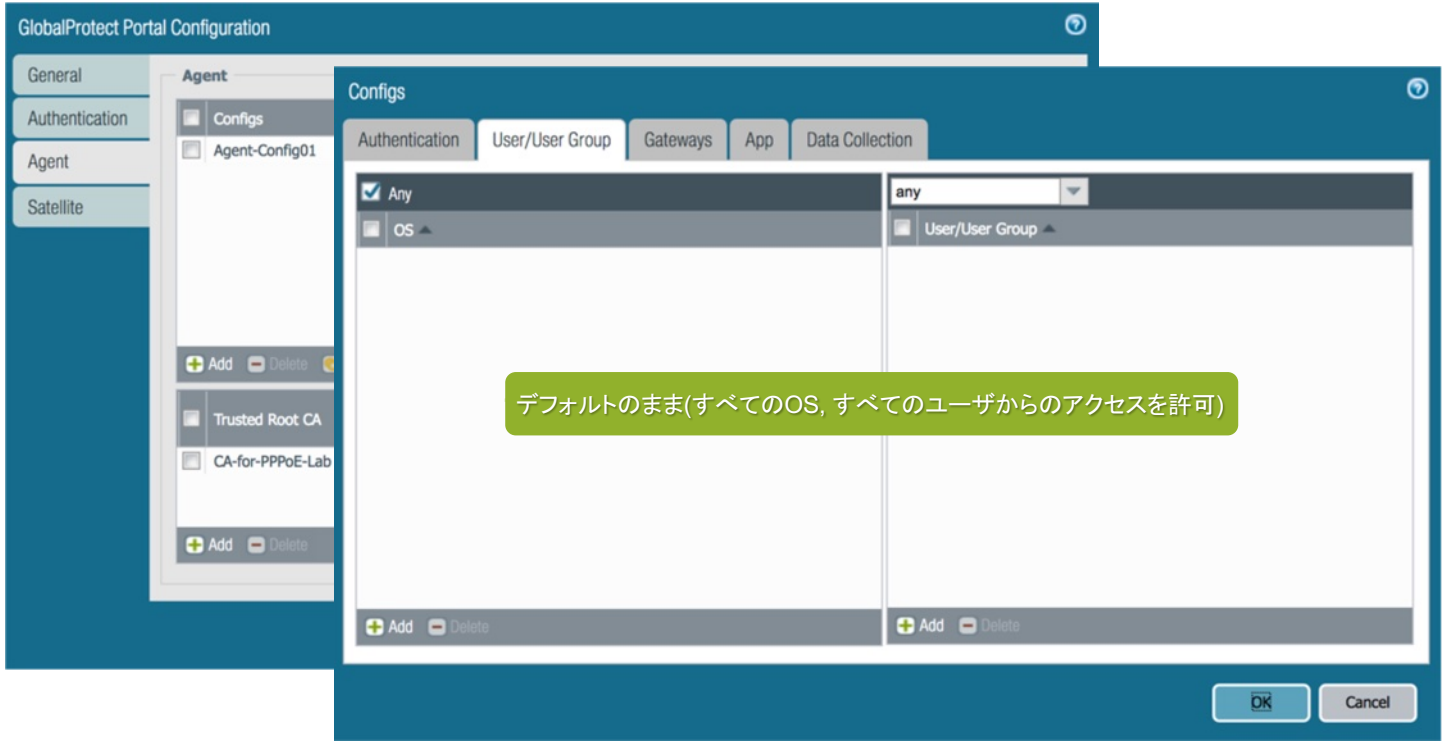
GlobalProtect ポータル 設定

- GP ポータルの設定 (Network > GlobalProtect > Portals)



GlobalProtect ポータル 設定

- GP ポータルの設定 (Network > GlobalProtect > Portals)



GlobalProtect ポータル 設定

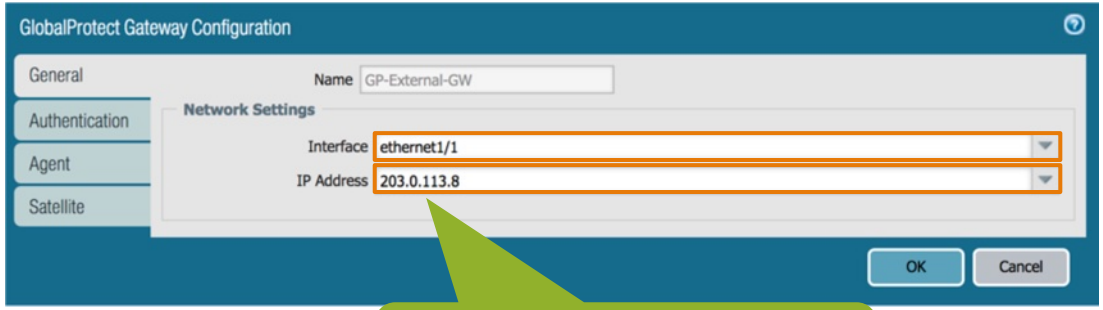
- GP ポータルの設定 (Network > GlobalProtect > Portals)

GlobalProtect ポータル 設定

- GP ポータルの設定 (Network > GlobalProtect > Portals)

GlobalProtect ゲートウェイ 設定

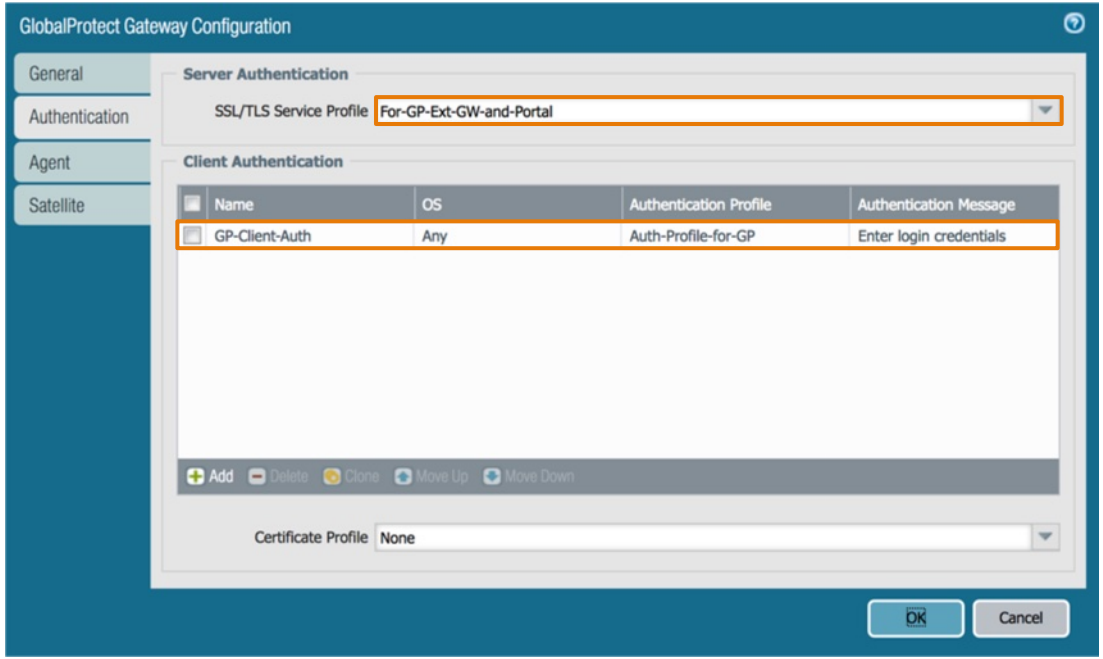
- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways > Add)



PPPoEを使用するLAN IFにIPアドレスを設定することで、GlobalProtect ゲートウェイで使用するIP アドレスの指定が出来る様になる

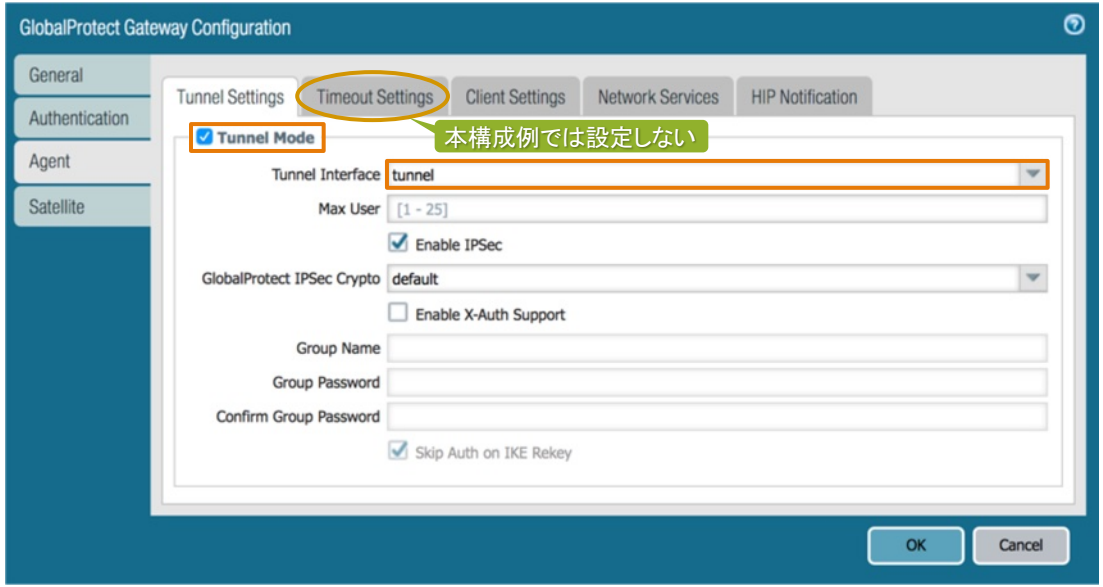
GlobalProtect ゲートウェイ 設定

- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways)



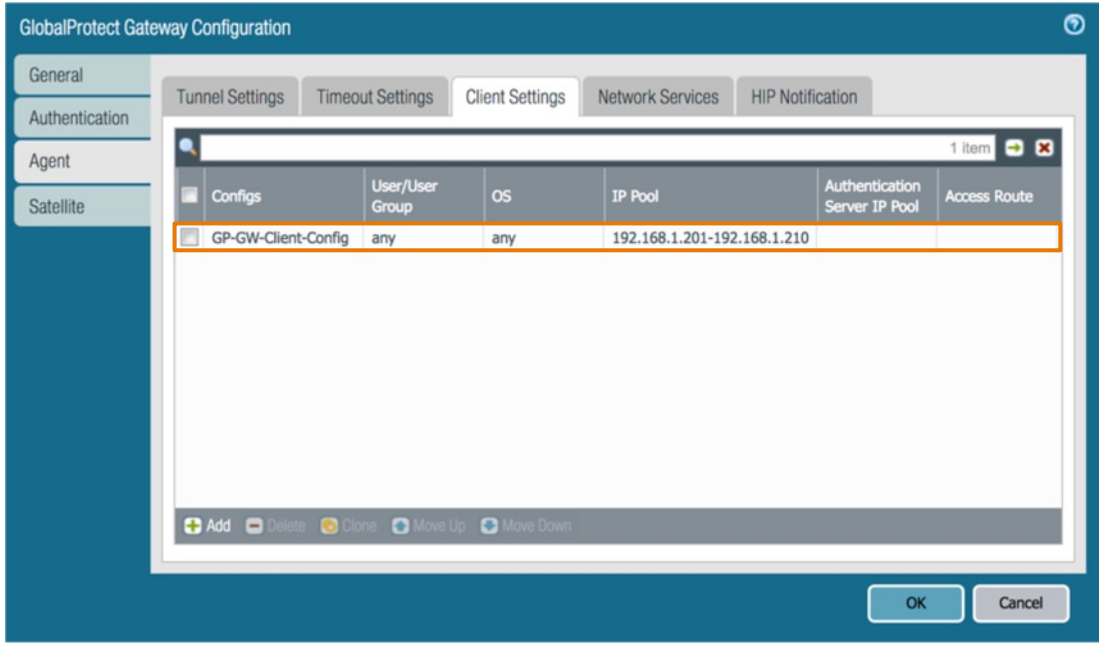
GlobalProtect ゲートウェイ 設定

- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways)



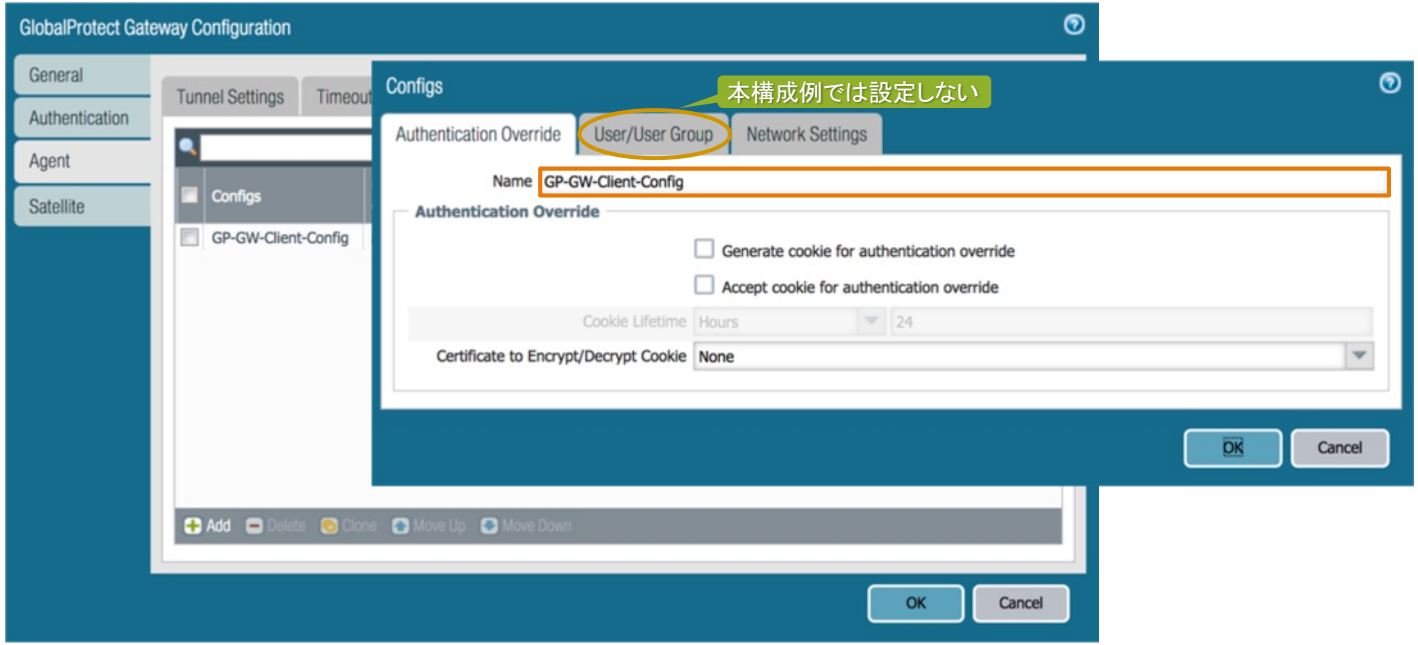
GlobalProtect ゲートウェイ 設定

- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways > Add)



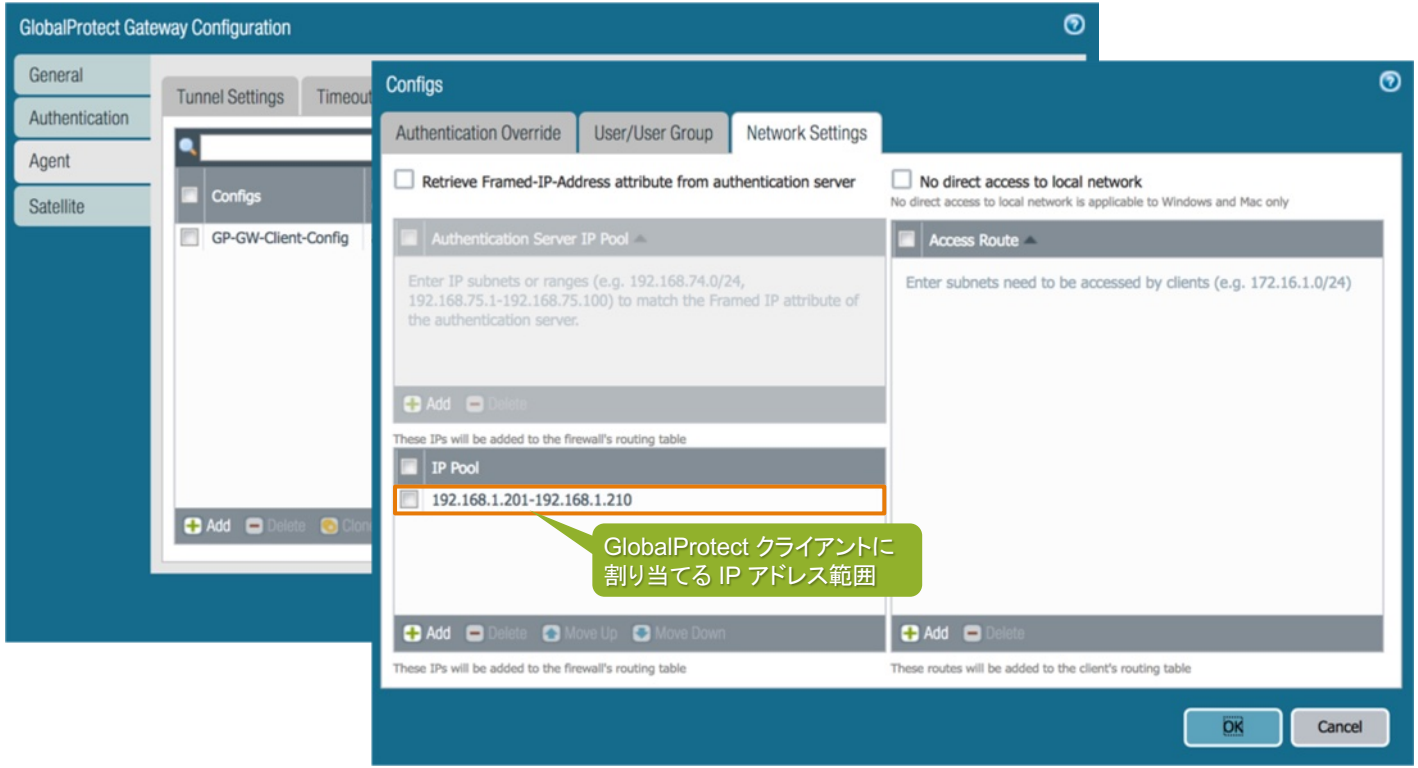
GlobalProtect ゲートウェイ 設定

- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways > Add)



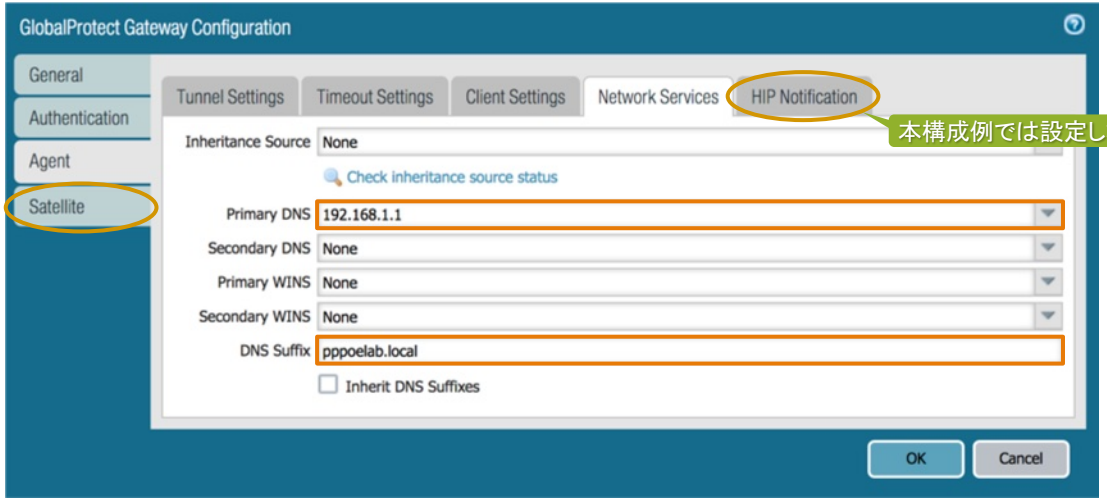
GlobalProtect ゲートウェイ 設定

- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways > Add)



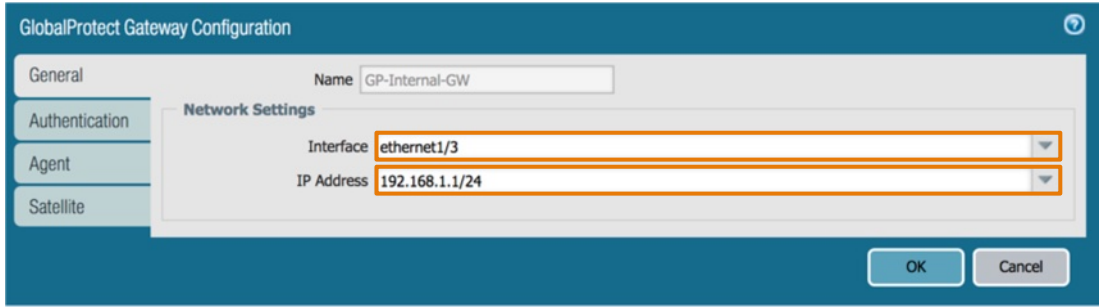
GlobalProtect ゲートウェイ 設定

- GP 外部ゲートウェイの設定 (Network > GlobalProtect > Gateways > Add)



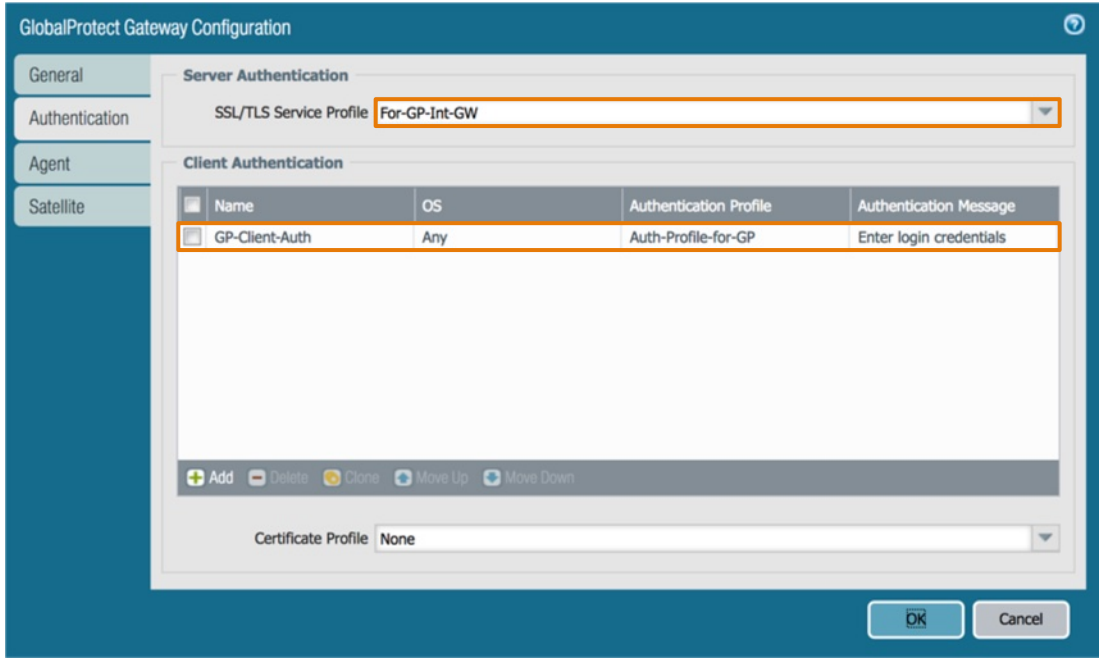
GlobalProtect ゲートウェイ 設定

- GP 内部ゲートェイの設定 (Network > GlobalProtect > Gateways > Add)



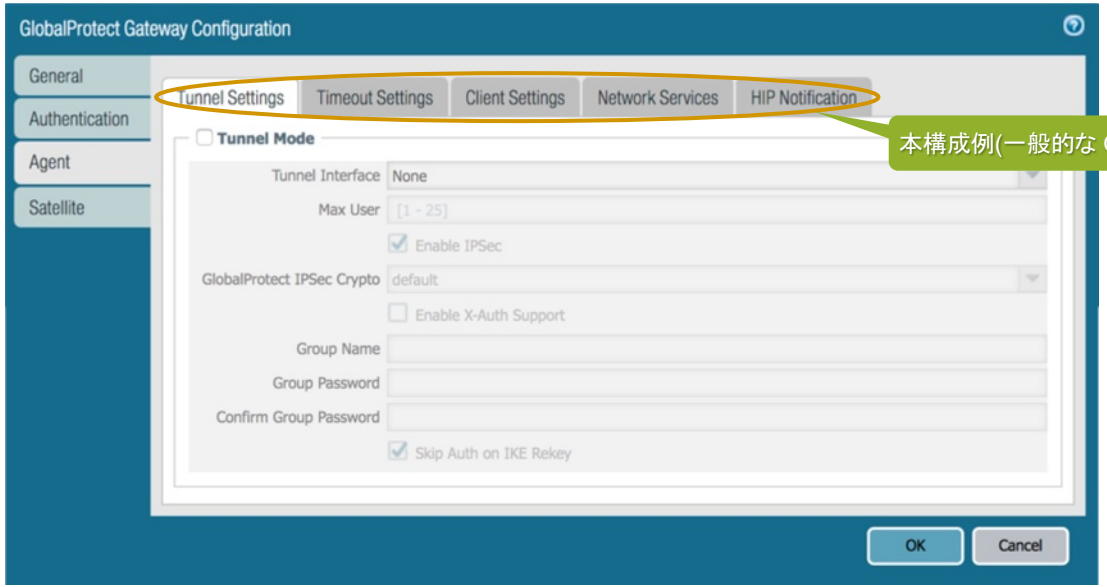
GlobalProtect ゲートウェイ 設定

- GP 内部ゲートェイの設定 (Network > GlobalProtect > Gateways > Add)



GlobalProtect ゲートウェイ 設定

- GP 内部ゲートェイの設定 (Network > GlobalProtect > Gateways > Add)



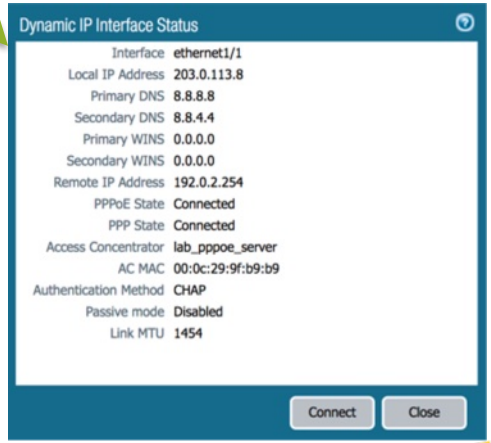
本構成例(一般的な GlobalProtect Internal Gateway構成)では設定しない

ネットワークインターフェイス設定一覧

- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

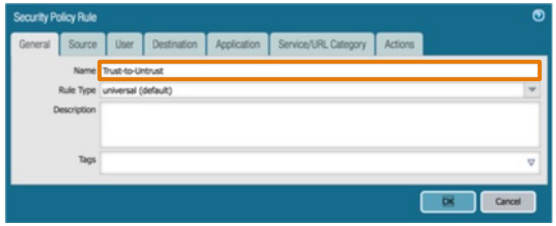
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone	Features
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	default	Untagged	L3-Untrust	
ethernet1/2				none	none	Untagged	none	
ethernet1/3	Layer3	ping-only		192.168.1.1/24	default	Untagged	L3-Trust	IP DNS

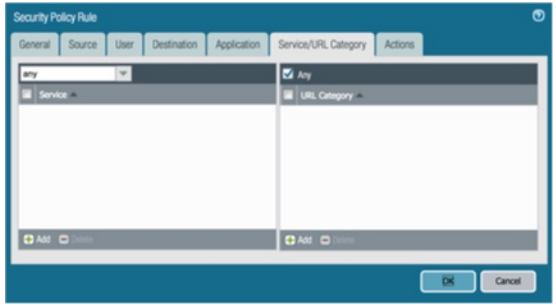
Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	default	L3-GP-Clients		

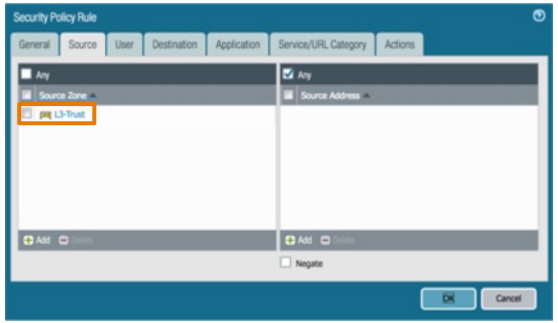


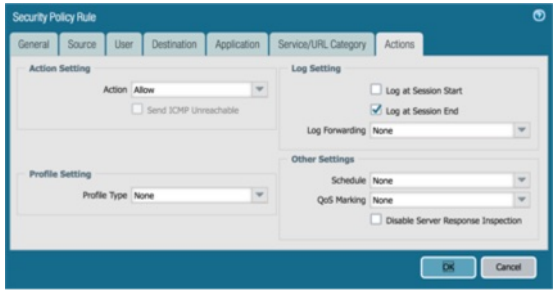
セキュリティポリシー設定

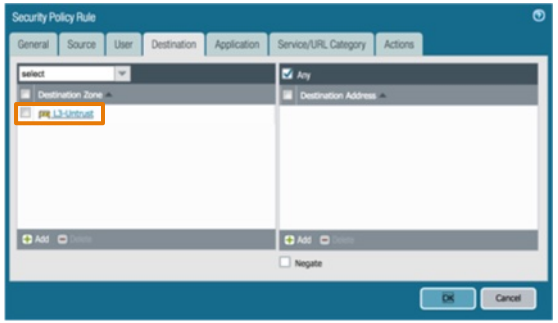
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security > Add)





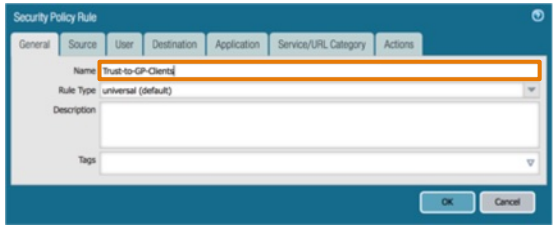


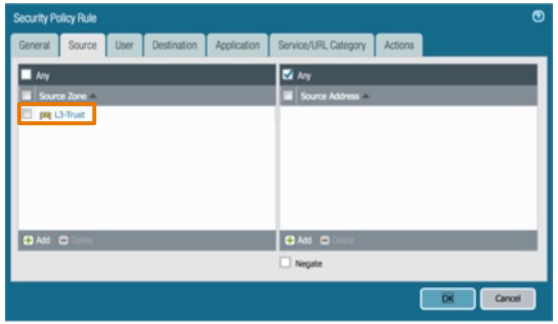


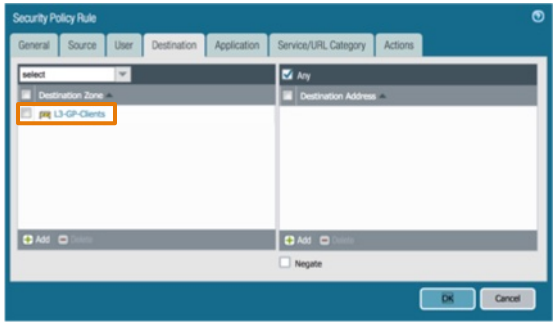


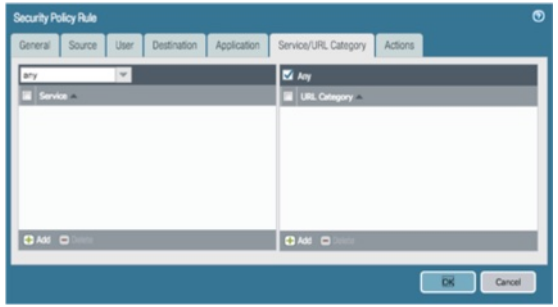
セキュリティポリシー設定

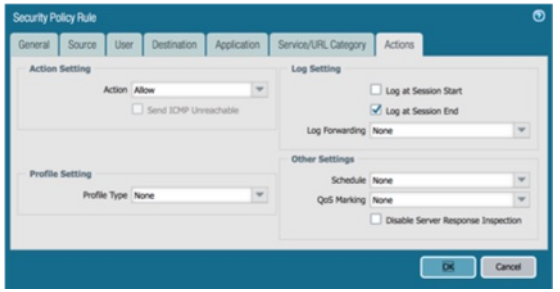
- 内部→GPクライアント通信用セキュリティポリシーの設定 (Policies > Security > Add)





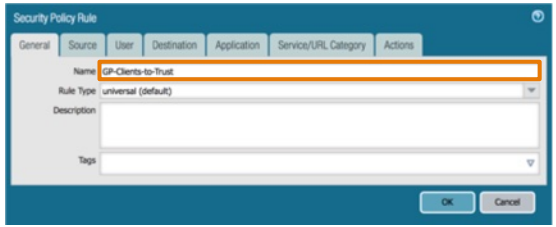


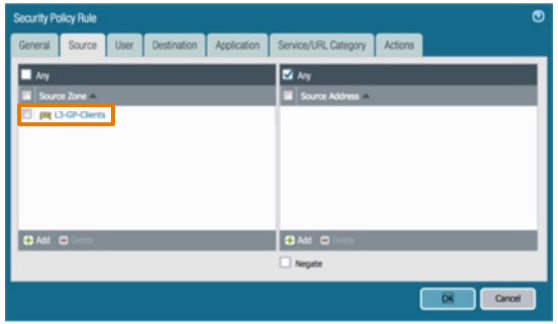


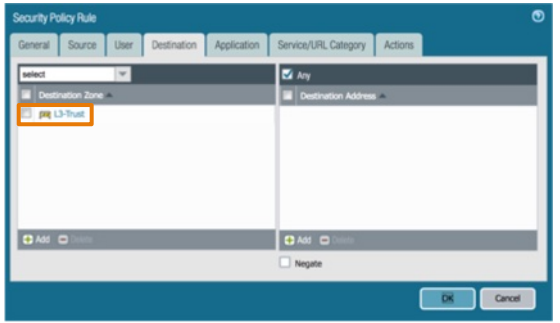


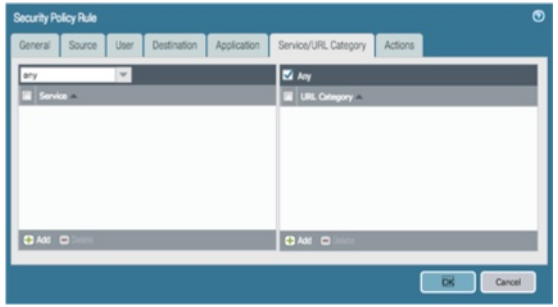
セキュリティポリシー設定

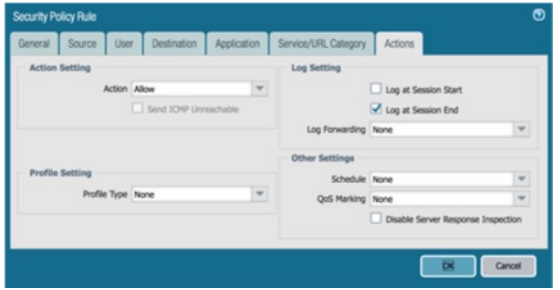
- GPクライアント→内部通信用セキュリティポリシーの設定 (Policies > Security > Add)





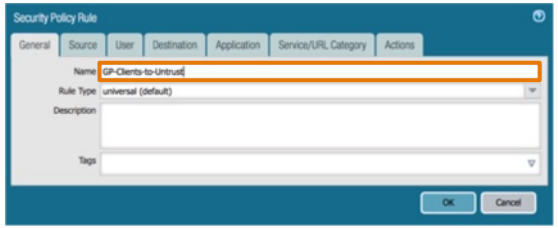


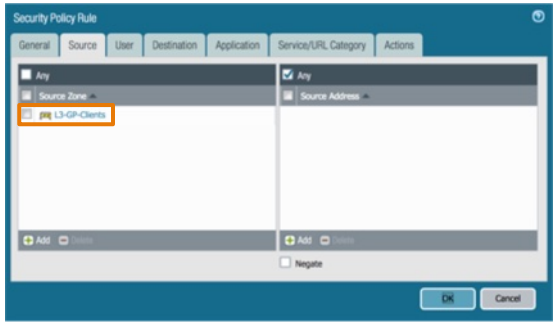


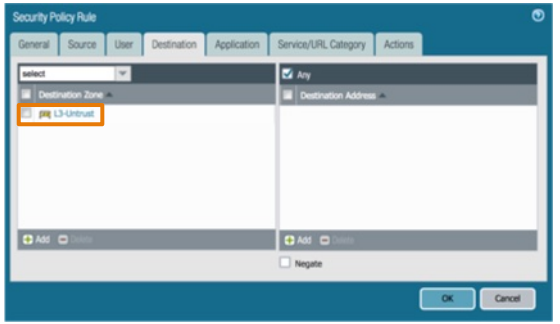


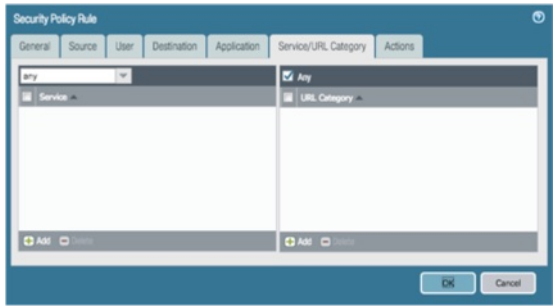
セキュリティポリシー設定

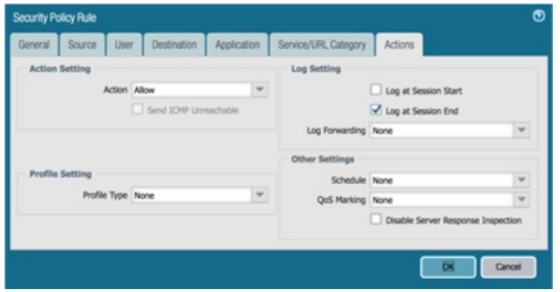
- GPクライアント→インターネット通信用セキュリティポリシーの設定 (Policies > Security > Add)











セキュリティポリシー設定一覧

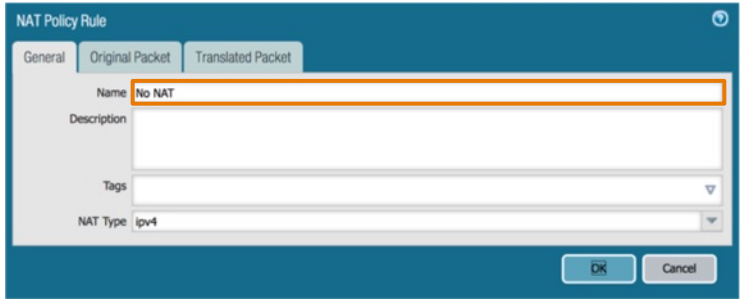
- セキュリティポリシー設定一覧 (Policies > Security)

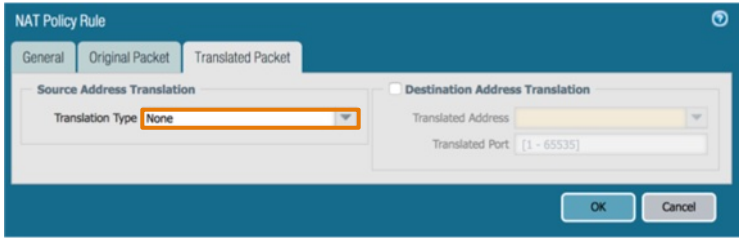
				Source			Destination						
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
2	Trust-to-GP-Clients	none	universal	L3-Trust	any	any	L3-GP-Clients	any	any	any	Allow	none	
3	GP-Clients-to-Trust	none	universal	L3-GP-Clients	any	any	L3-Trust	any	any	any	Allow	none	
4	GP-Clients-to-Untrust	none	universal	L3-GP-Clients	any	any	L3-Untrust	any	any	any	Allow	none	
5	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
6	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

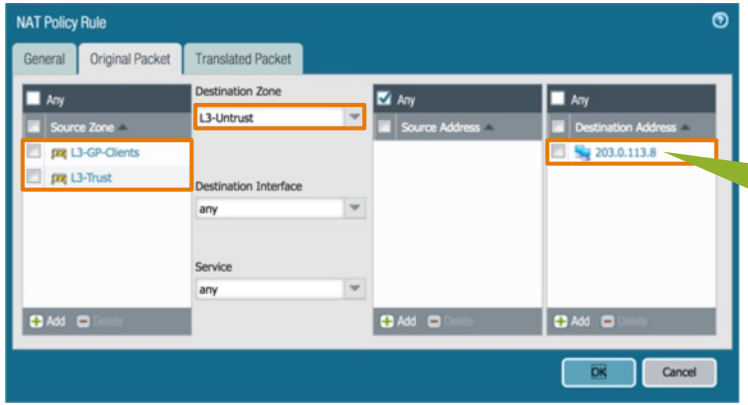
NATポリシー設定

させない

- 内部 → GP 外部ポータル, ゲートウェイ IP 向けNATポリシーの設定 (Policies > NAT)





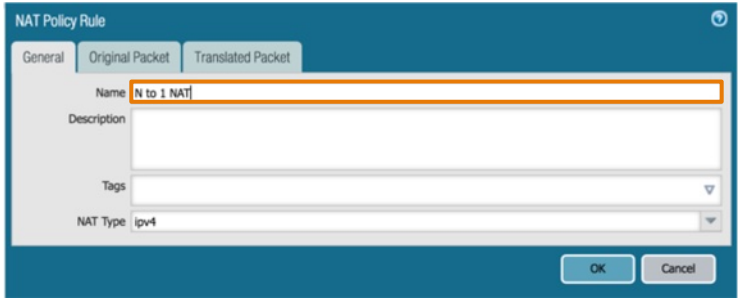


PAの(PPPoE 接続されている)インターネット側インターフェイス IP アドレス
※PAは内部ネットワーク側から外部側のインターフェイスアドレスに設定された
IPアドレスに対して通信する場合 NAT処理を無効化しなければならない

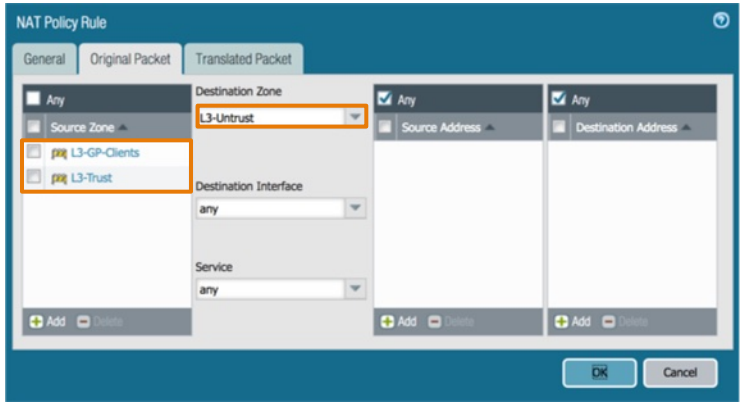
 |

NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)



IPアドレスは指定しなくて良い
(インターフェイス に割当てられた
IPアドレスが自動的に使われる)



NATポリシー設定一覧

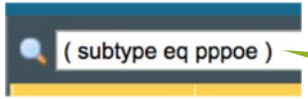
- NATポリシー設定一覧 (Policies > NAT)

		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	No NAT	L3-GP-Clients L3-Trust	L3-Untrust	any	any	203.0.113.8	any	none	none
2	N to 1 NAT	L3-GP-Clients L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

設定後のPPPoE 接続ログ例

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/26 17:01:10	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:5, IP Address negotiated:203.0.113.8
03/26 17:01:06	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:fixed-ip-user1@pppoelab.local on interface:ethernet1/1



表示フィルタを使用することで必要なログを素早く確認することが可能

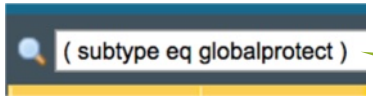
設定後の**GlobalProtect** 接続ログ例

- GlobalProtect 外部ゲートウェイ接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/27 17:22:23	globalprotect	informational	globalprotectgateway-config-succ	GP-External-GW-N	GlobalProtect gateway client configuration generated. User name: GPuser01, Private IP: 192.168.1.202, Client version: 4.0.7-5, Device name: WIN7PRO-X64-02, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, VPN type: Device Level VPN.
03/27 17:22:23	globalprotect	informational	globalprotectgateway-regist-succ	GP-External-GW-N	GlobalProtect gateway user login succeeded. Login from: 198.51.100.120, User name: GPuser01, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.
03/27 17:22:22	globalprotect	informational	globalprotectgateway-auth-succ	GP-External-GW-N	GlobalProtect gateway user authentication succeeded. Login from: 198.51.100.120, User name: GPuser01, Auth type: profile, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.
03/27 17:22:22	globalprotect	informational	globalprotectportal-config-succ	GP-Portal	GlobalProtect portal client configuration generated. Login from: 198.51.100.120, User name: GPuser01, Config name: Agent-Config01.
03/27 17:22:21	globalprotect	informational	globalprotectportal-auth-succ	GP-Portal	GlobalProtect portal user authentication succeeded. Login from: 198.51.100.120, User name: GPuser01, Auth type: profile.

<ログアウト時> *OSシャットダウン操作時

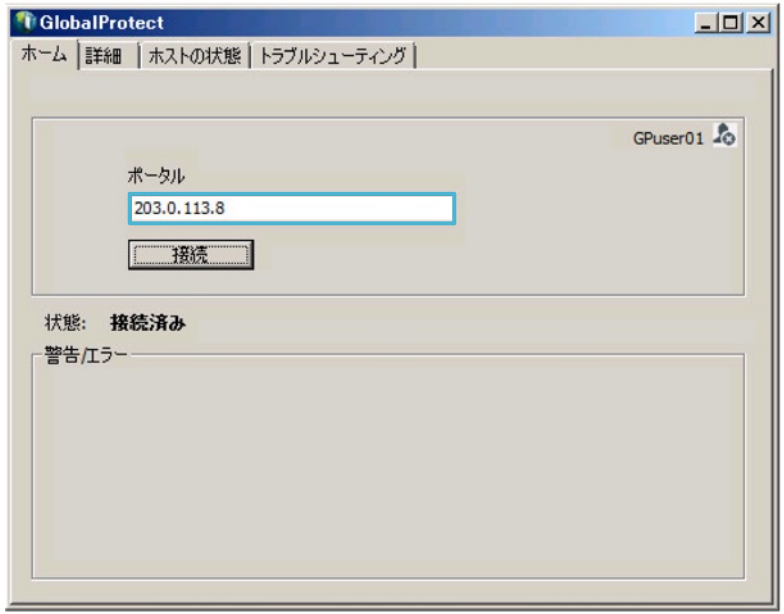
Receive Time	Type	Severity	Event	Object	Description
03/27 17:27:32	globalprotect	informational	globalprotectgateway-logout-succ	GP-External-GW-N	GlobalProtect gateway user logout succeeded. User name: GPuser01, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, Reason: client logout.

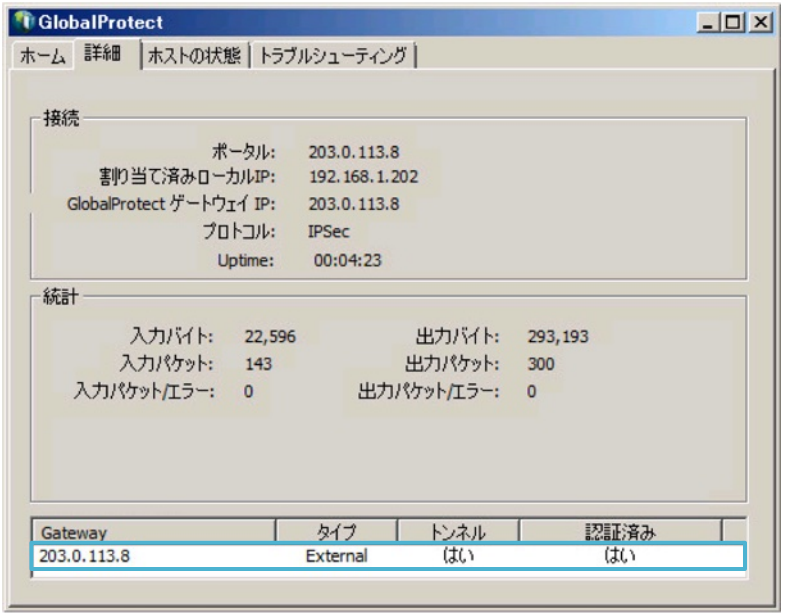


表示フィルタを使用することで必要なログを素早く確認することが可能

設定後のGlobalProtect クライアント画面例 (外部GW接続時)

- GlobalProtect 外部ゲートウェイ接続時の GPクライアントアプリケーション画面例





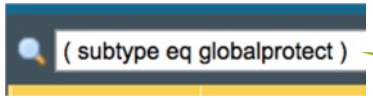
設定後のGlobalProtect 接続ログ例

- GlobalProtect 内部ゲートウェイ接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/27 17:15:39	globalprotect	informational	globalprotectgateway-config-release	GP-Internal-GW	GlobalProtect gateway client configuration released. User name: GPuser01, Public IP: 192.168.1.102, Client version: , Device name: WIN7PRO-X64-02, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, VPN type: Device Level VPN.
03/27 17:10:42	globalprotect	informational	globalprotectgateway-regist-succ	GP-Internal-GW	GlobalProtect gateway user login succeeded. Login from: 192.168.1.102, User name: GPuser01, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.
03/27 17:10:42	globalprotect	informational	globalprotectgateway-auth-succ	GP-Internal-GW	GlobalProtect gateway user authentication succeeded. Login from: 192.168.1.102, User name: GPuser01, Auth type: profile, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.
03/27 17:10:41	globalprotect	informational	globalprotectportal-config-succ	GP-Portal	GlobalProtect portal client configuration generated. Login from: 192.168.1.102, User name: GPuser01, Config name: Agent-Config01.
03/27 17:10:41	globalprotect	informational	globalprotectportal-auth-succ	GP-Portal	GlobalProtect portal user authentication succeeded. Login from: 192.168.1.102, User name: GPuser01, Auth type: profile.

<ログアウト時> *OSをシャットダウン

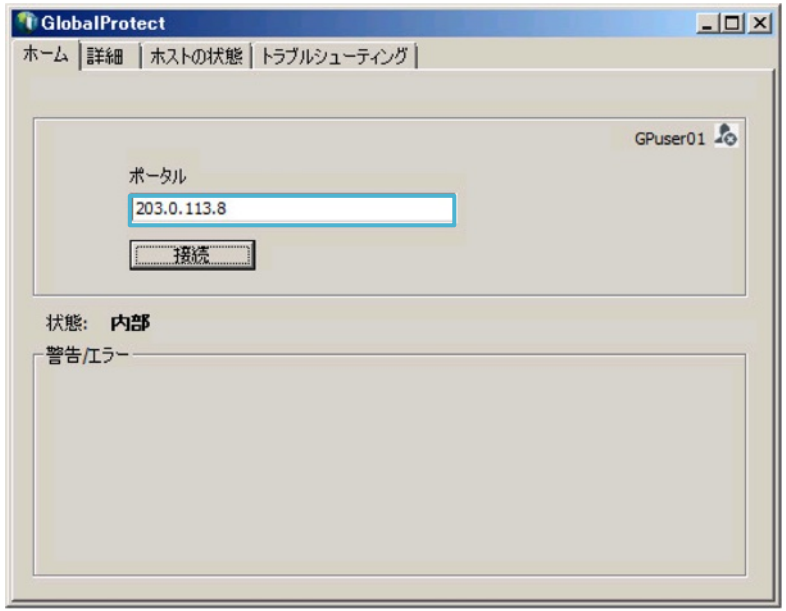
Receive Time	Type	Severity	Event	Object	Description
03/27 17:15:39	globalprotect	informational	globalprotectgateway-logout-succ	GP-Internal-GW	GlobalProtect gateway user logout succeeded. User name: GPuser01, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, Reason: client logout.

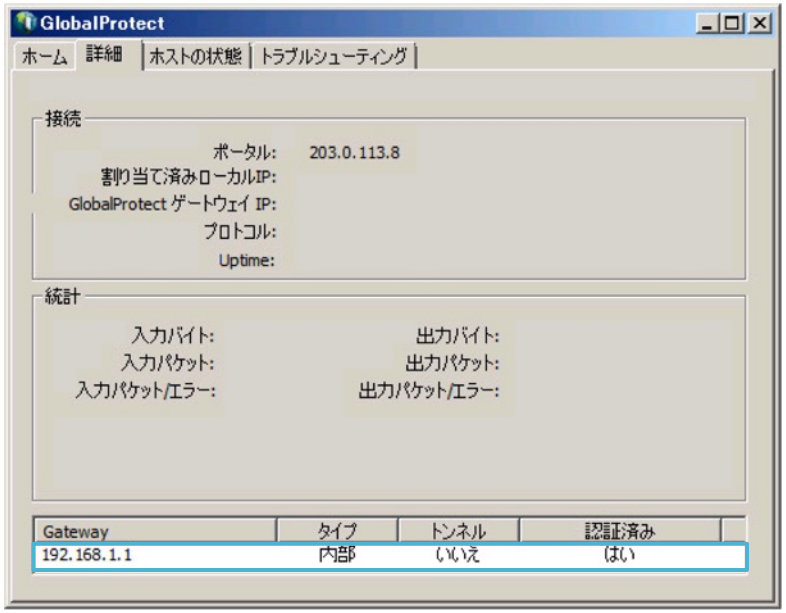


表示フィルタを使用することで必要なログを素早く確認することが可能

設定後のGlobalProtect クライアント画面例 (内部GW接続時)

- GlobalProtect 内部ゲートウェイ接続時の GPクライアントアプリケーション画面

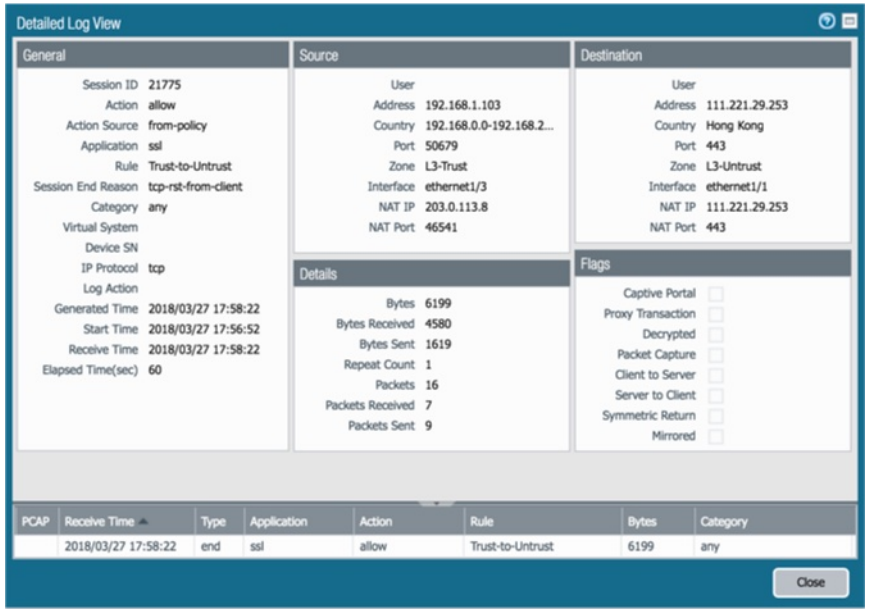




設定後のトラフィックログ例

- 内部からインターネットへ通信した場合のログ例 (Monitor > Logs > Traffic)

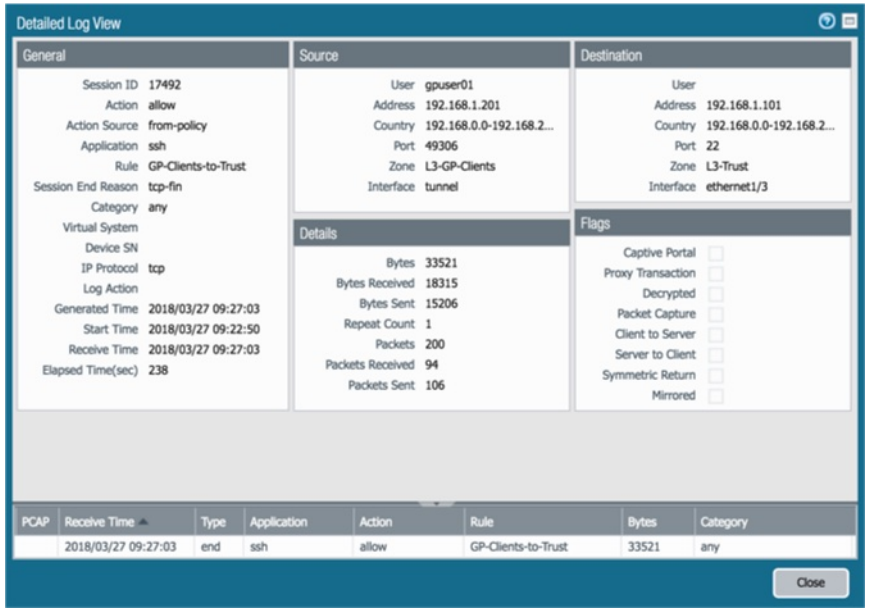
		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/27 17:58:22	end	L3-Trust	L3-Untrust	192.168.1.103		111.221.29.253	443	ssl	any	allow	Trust-to-Untrust	tcp-rst-from-client	6.2k



設定後のトラフィックログ例

- GlobalProtect クライアントから内部へ通信した場合のログ例 (Monitor > Logs > Traffic)

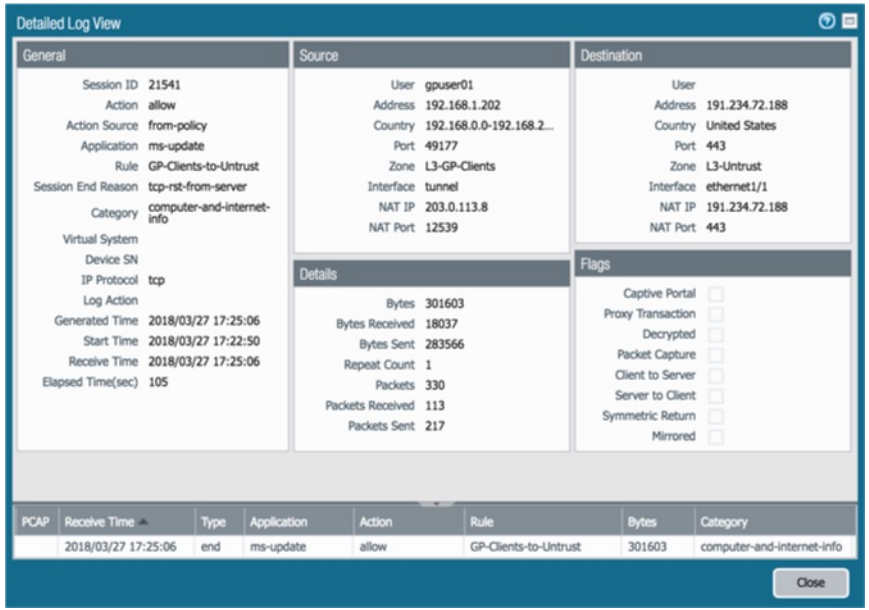
		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/27 09:27:03	end	L3-GP-Clients	L3-Trust	192.168.1.201	gpuser01	192.168.1.101	22	ssh	any	allow	GP-Clients-to-Trust	tcp-fin	33.5k



設定後のトラフィックログ例

- GlobalProtect クライアントからPA経由でインターネットへ通信した場合のログ例 (Monitor > Logs > Traffic)

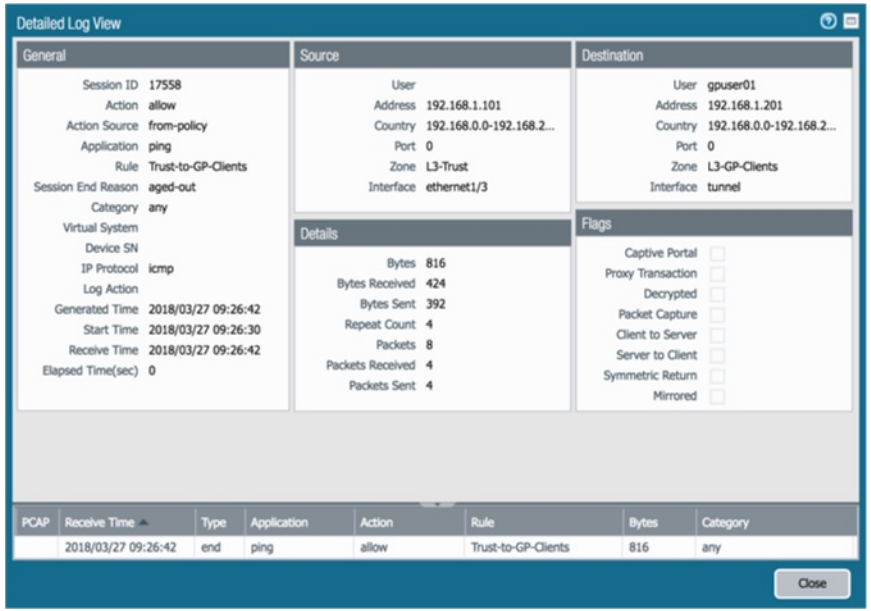
		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/27 17:25:06	end	L3-GP-Clients	L3-Untrust	192.168.1.202	gpuser01	191.234.72.188	443	ms-update	computer-and-internet-info	allow	GP-Clients-to-Untrust	tcp-rst-from-server	301.6k



設定後のトラフィックログ例

- 内部からGlobalProtect クライアントへ通信した場合のログ例 (Monitor > Logs > Traffic)

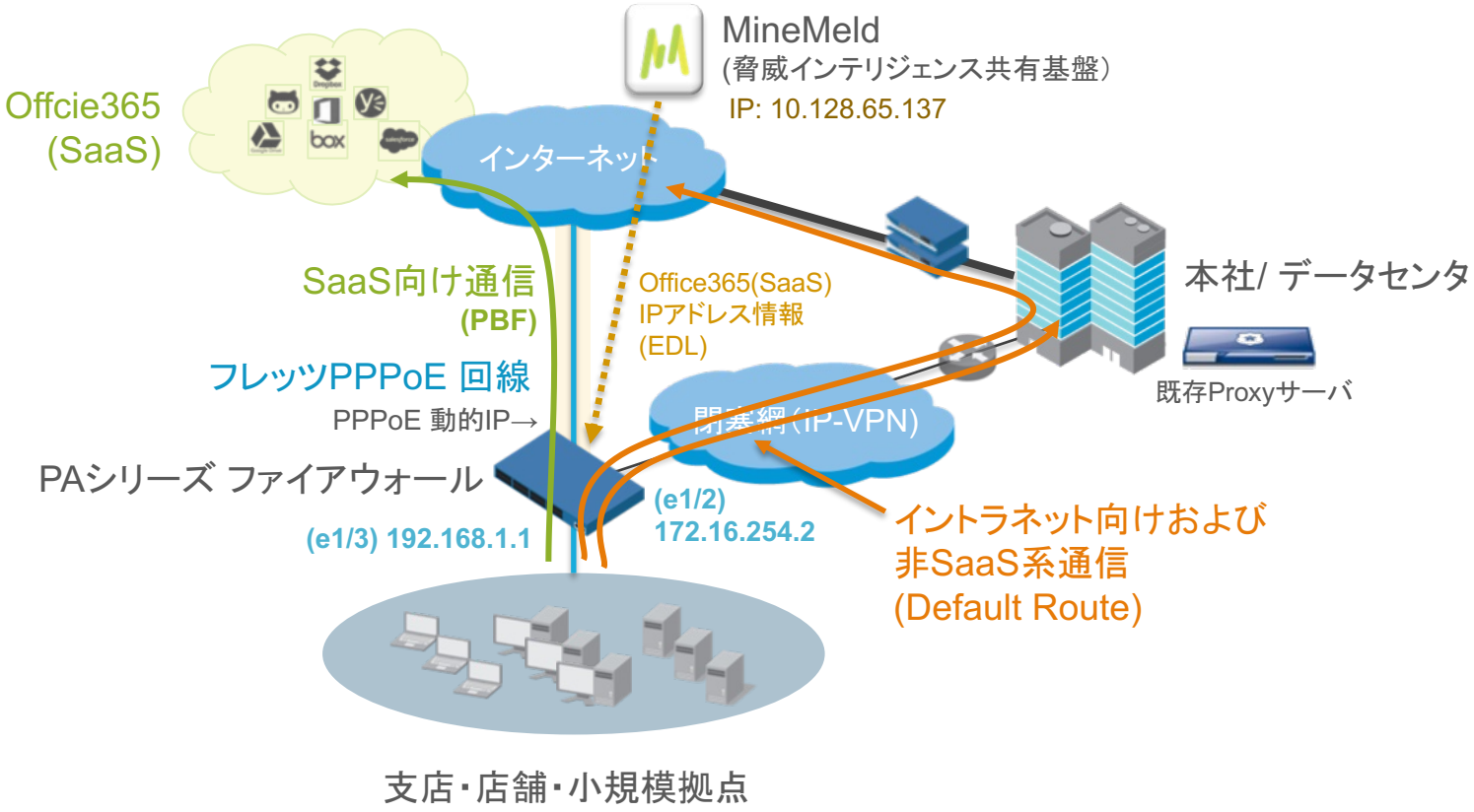
		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/27 09:26:42	end	L3-Trust	L3-GP-Clients	192.168.1.101		192.168.1.201	0	ping	any	allow	Trust-to-GP-Clients	aged-out	816



PPPoE 設定例６

MineMeld, PBF(ポリシーベースフォワーディング)
による Office365(SaaS)トラフィックの分離
(ローカルブレイクアウト構成)

設定例6:



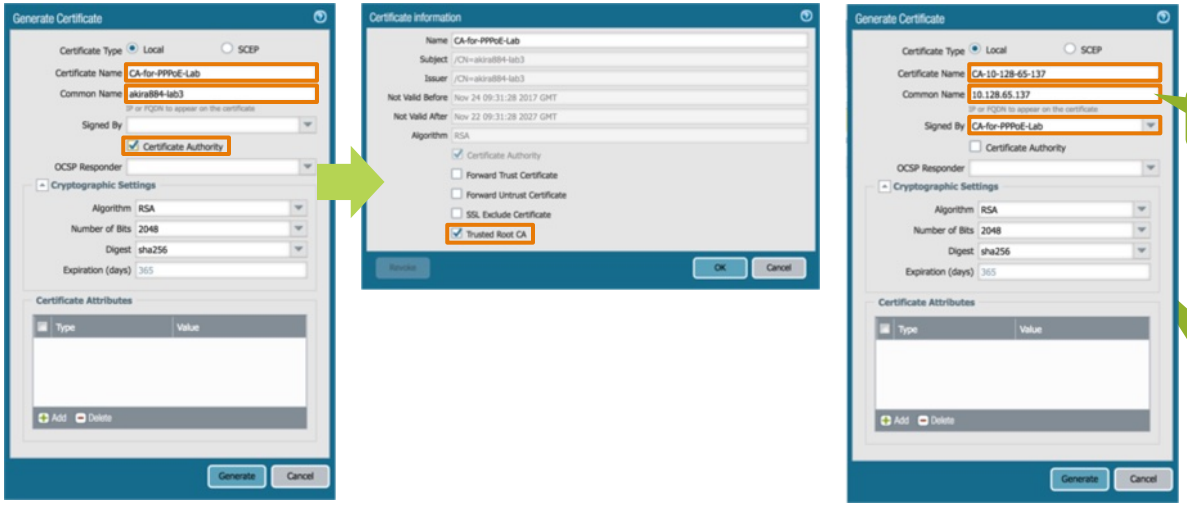
コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE関連	・MTU 値を必ず変更する。(例:1454) ・PPPoE 認証方式はデフォルトのままで問題なし。
その他	・AutoFocus上のMineMeld を使用する場合(推奨)は PAN-OS 8.0 以上のバージョンをご利用下さい。 ・Office 365 のグローバル IPアドレス情報はマイクロソフト社の公開情報を元にしており、完全なトラフィック分離を保証するものではありません。またOffice365に関連するアプリケーショントラフィックがトラフィック分離の対象になる可能性があります。(MineMeld/PAはマイクロソフト社の情報に沿って動作します) 参考URL: https://support.office.com/ja-jp/article/office-365-url-および-ip-アドレス範囲-8548a211-3fe7-47cb-abb1-355ea5aa88a2 ・本番環境において使用する CA証明書、MineMeld用サーバ証明書は、組織で利用している証明書サービスなどで発行されたものをご利用下さい。

☆実環境においては、各種脅威防御やURLフィルタリング WildFireなど、重要なセキュリティ機能を必ず設定・ご利用下さい。

MineMeld SSL接続用 サーバ証明書の生成

- MineMeldが稼働しているWebサーバ用SSLサーバ証明書を生成
(Device > Certificate Management > Certificates > Generate)

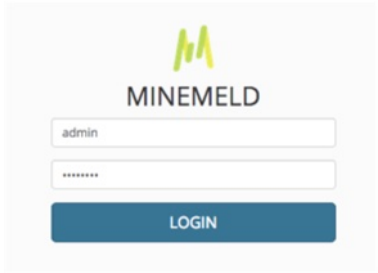


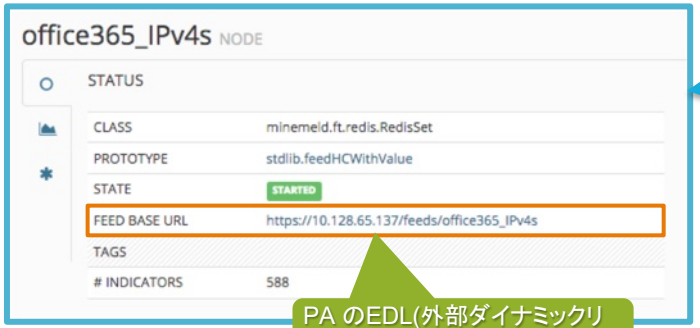
Name	Subject	Issuer	CA	K...	Expires	Sta...	Al...	Usage
CA-for-PPPoE-Lab	CN = akira884-lab3	CN = akira884-lab3	☑	☑	Nov 22 09:31:28 2027 GMT	valid	RSA	Trusted Root CA Certificate
CA-10-128-65-137	CN = 10.128.65.137	CN = akira884-lab3	☐	☑	Nov 22 09:34:25 2027 GMT	valid	RSA	

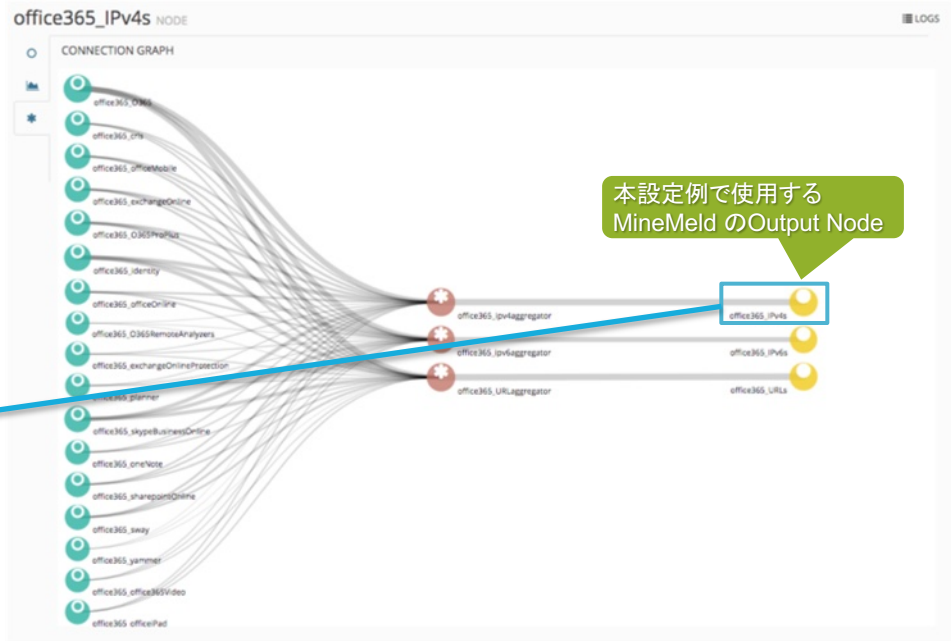
生成したSSLサーバ証明書をKeyと共にExportしMineMeld のWebサーバにインポートする

MineMeld の設定（参考）

- Office365 IPv4アドレス処理用 OUTPUT ノード “office365_IPv4s”の構成 (NODES > office365_IPv4s|OUTPUT)

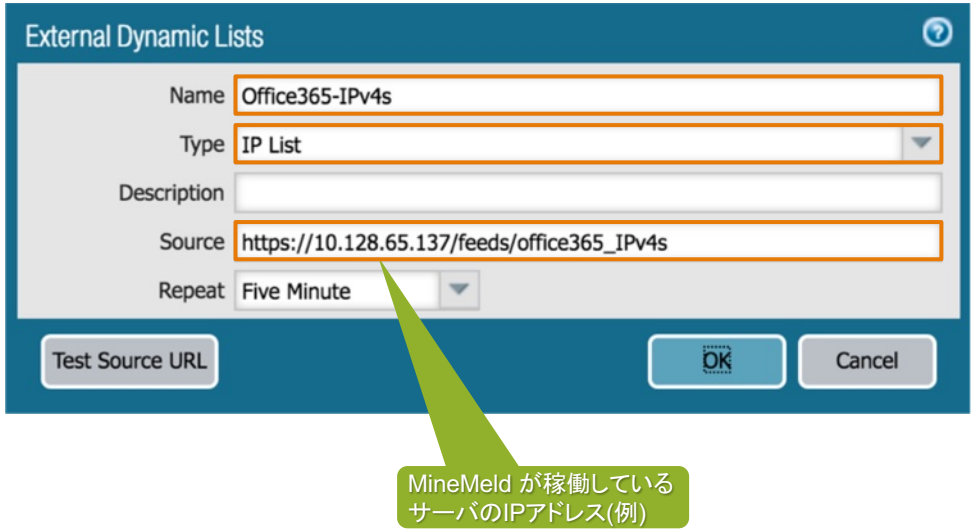






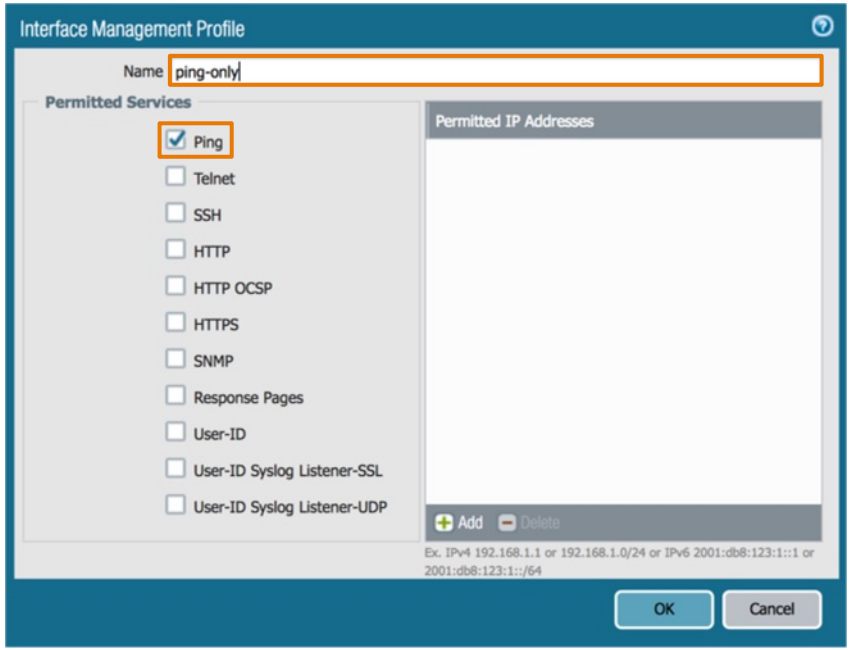
Office365 向けトラフィック制御用 外部ダイナミックリストの作成

- 外部ダイナミックリスト(EDL)の設定 (Objects > External Dynamic Lists > Add)



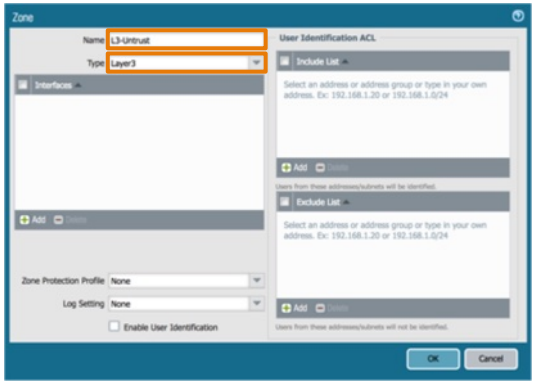
インターフェイス管理アクセス設定

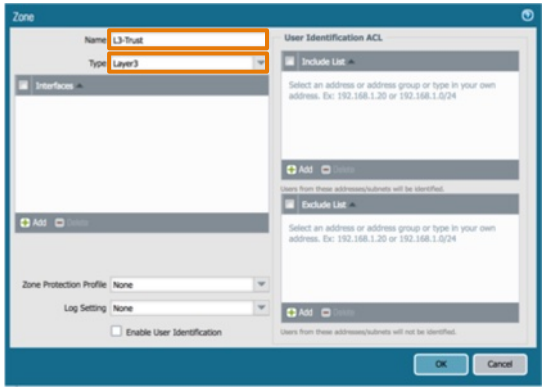
- データプレーン用インターフェイスへのpingを許可するためのプロファイル作成 (Network > Network Profiles > Interface Mgmt)

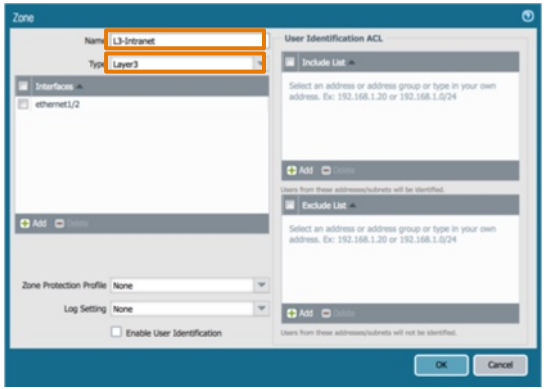


セキュリティゾーン設定

- 外部ネットワーク, 内部ネットワーク, イントラネット用セキュリティゾーンを作成 (Network > Zones)

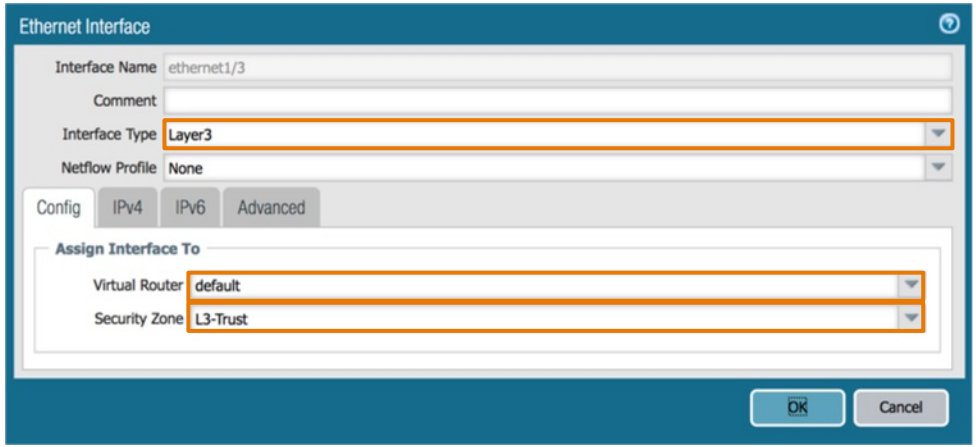






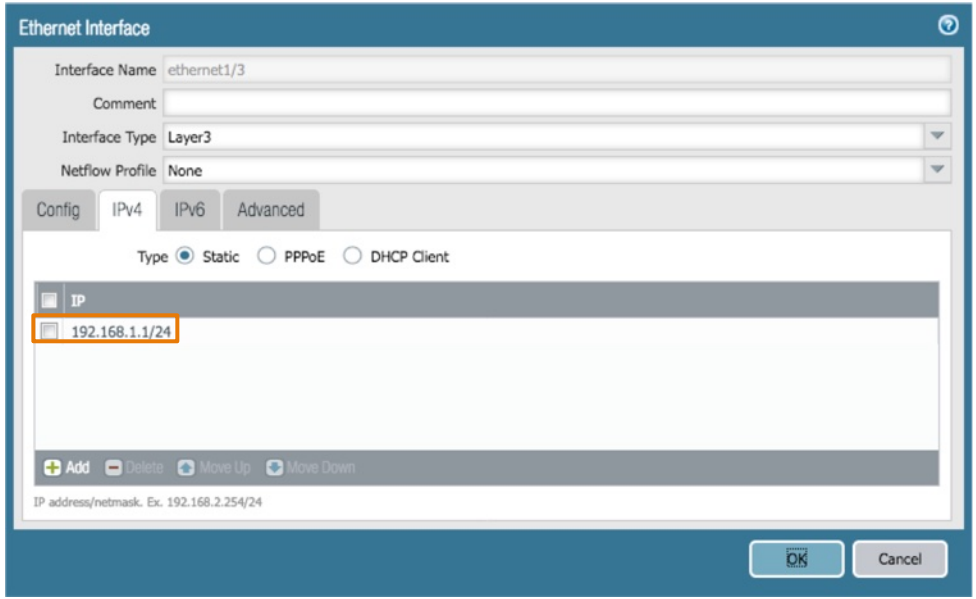
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



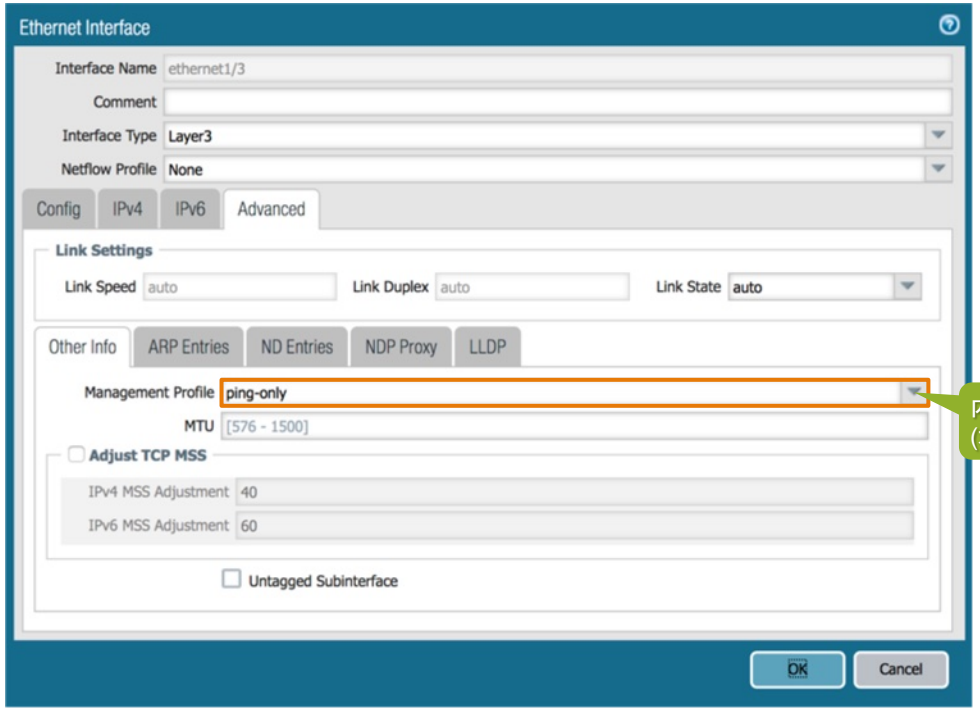
内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



内部ネットワーク用インターフェイス設定

- ethernet1/3 インターフェイスの設定 (Network > Interfaces)



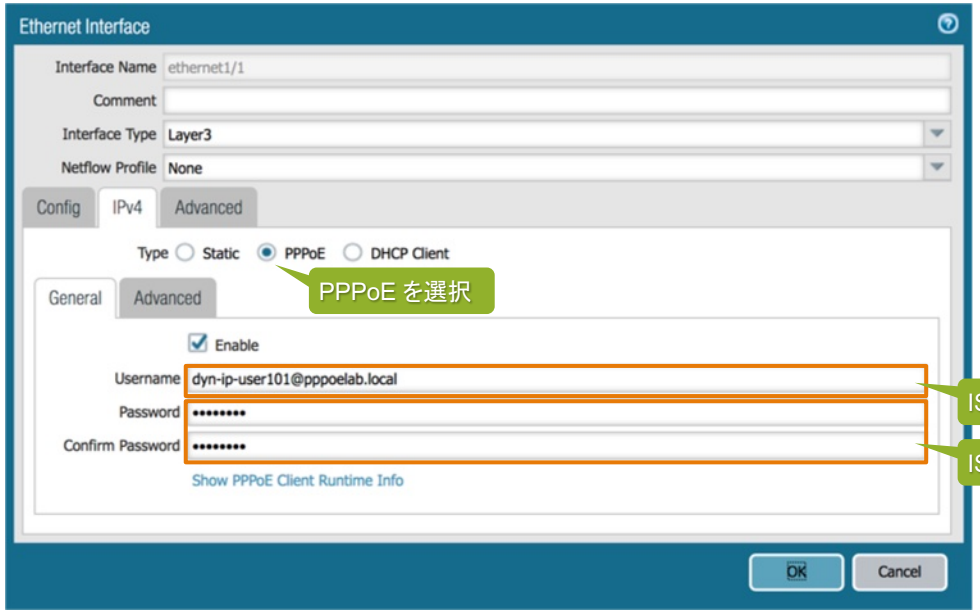
内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

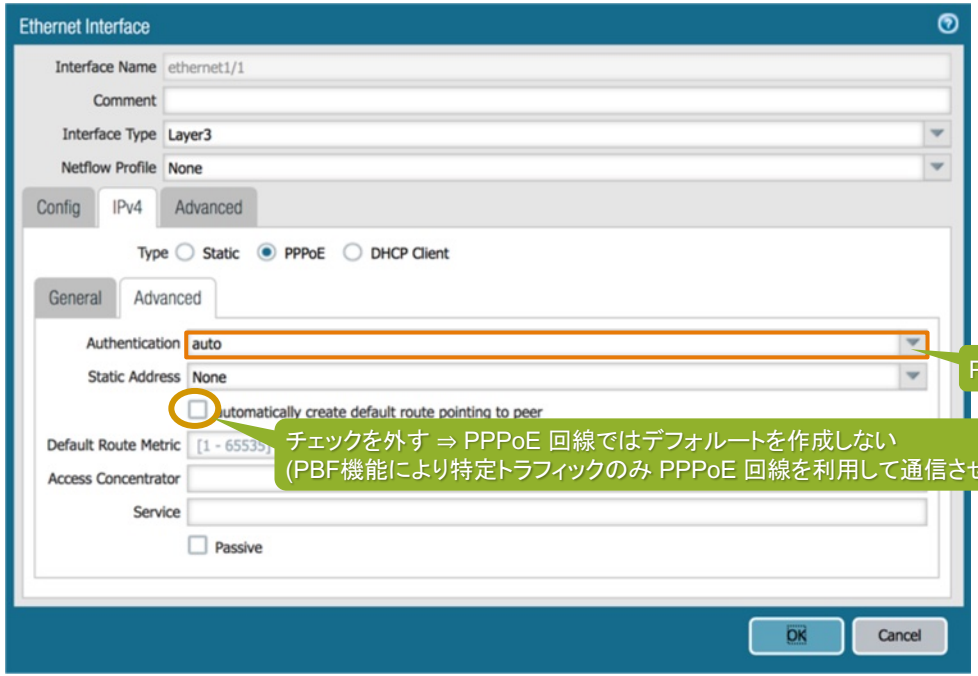


ISPから発行された PPPoE 回線接続用アカウントを入力

ISPから発行された PPPoE 回線接続用パスワードを入力

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

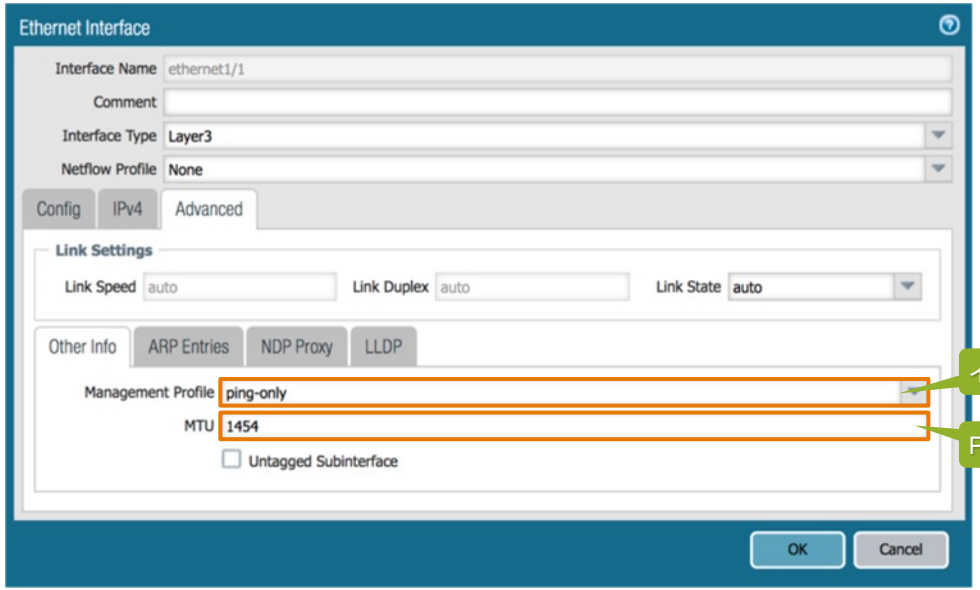


PPPoE 認証方式は自動のままで良い（CHAP/PAP共にサポート）

チェックを外す ⇒ PPPoE 回線ではデフォルートを作成しない
(PBF機能により特定トラフィックのみ PPPoE 回線を利用して通信させるため)

外部ネットワーク用インターフェイス設定

- ethernet1/1 インターフェイスの設定 (Network > Interfaces)

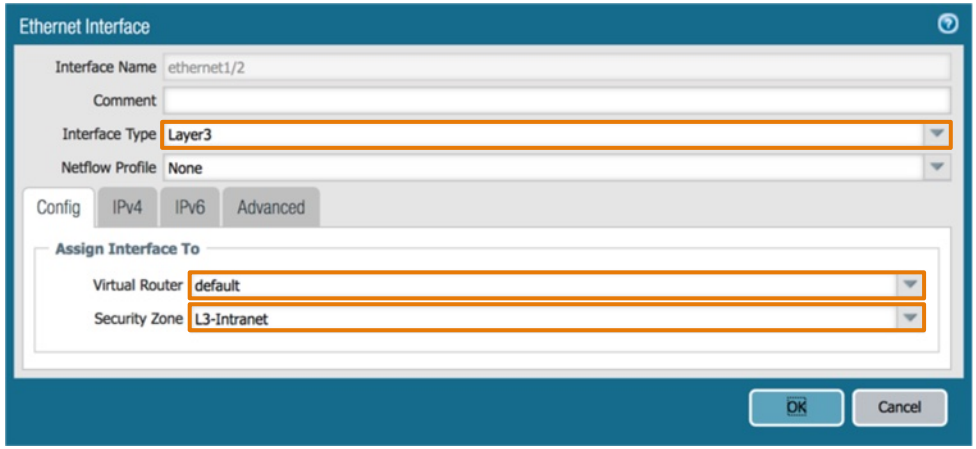


インターネット側からのICMPによる疎通確認のための設定 (オプション)

PPPoE を使用するインターフェイスのMTUは必ず変更する

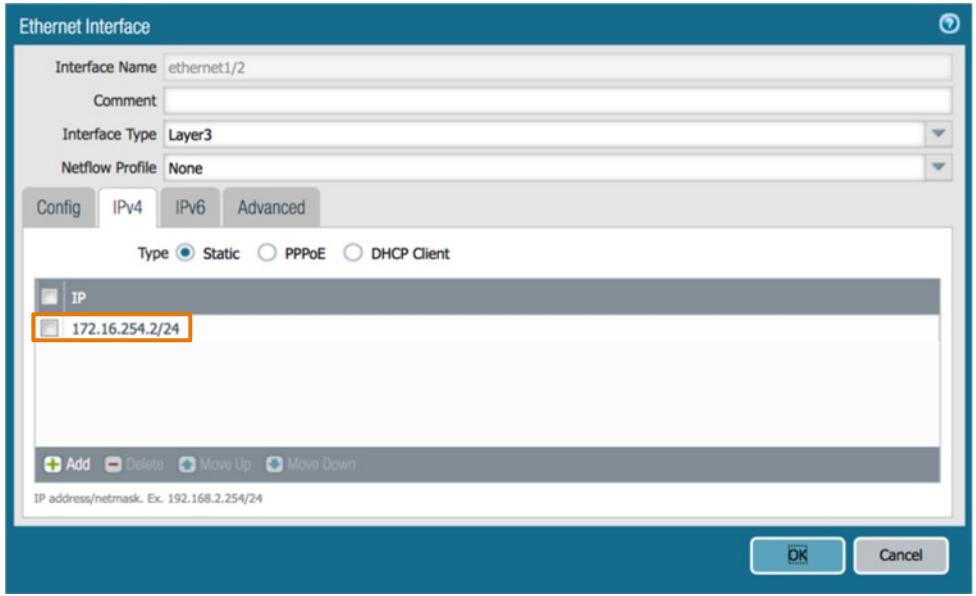
イントラネット接続用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



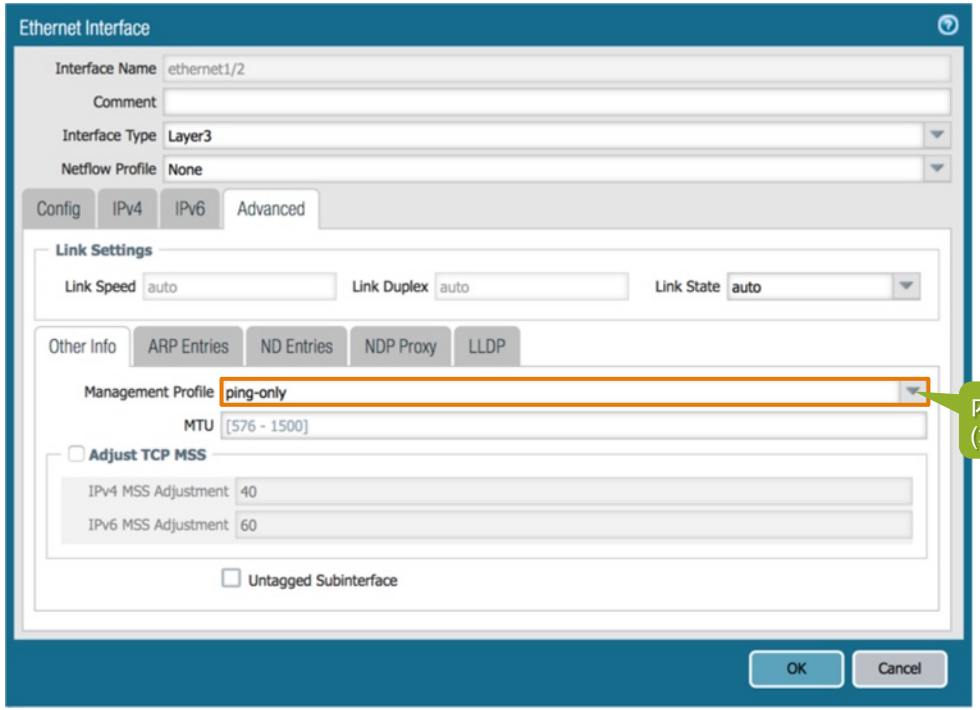
イントラネット接続用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)



イントラネット接続用インターフェイス設定

- ethernet1/2 インターフェイスの設定 (Network > Interfaces)

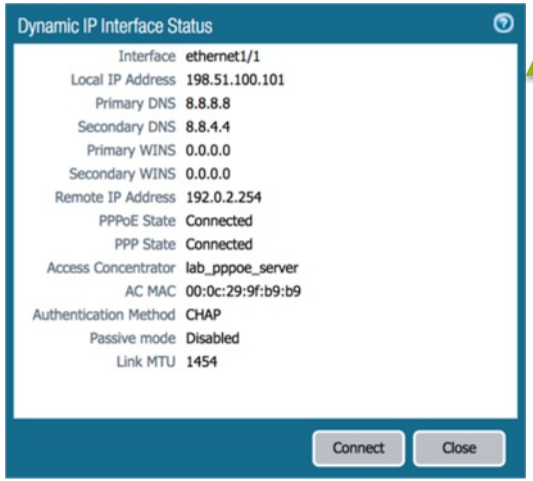


内部ネットワーク側からのICMPによる疎通確認のための設定(オプション)

ネットワークインターフェイス設定一覧

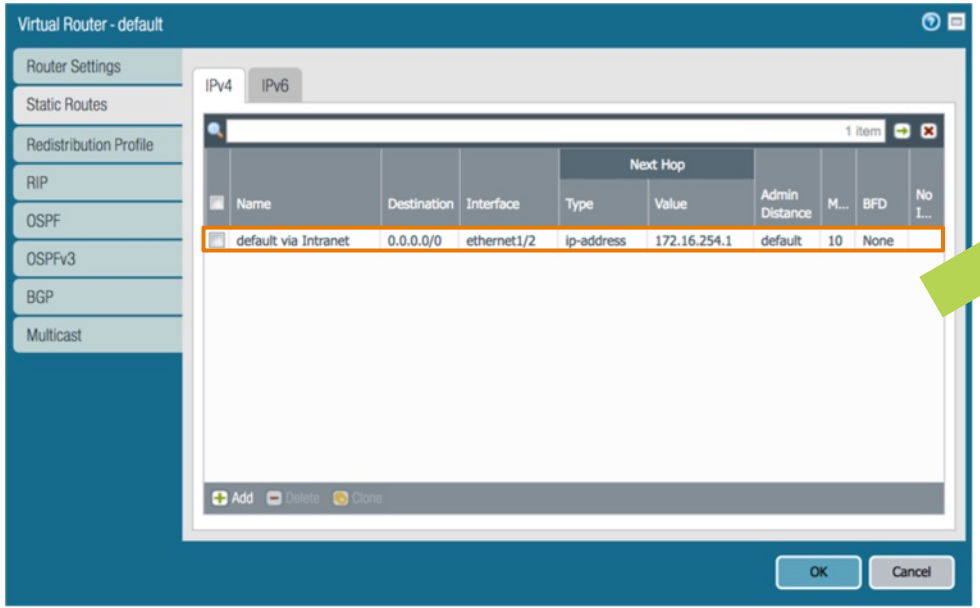
- インターフェイスの設定と PPPoE ステータス (Network > Interfaces)

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	Security Zone	Features
ethernet1/1	Layer3	ping-only		Dynamic-PPPoE	default	Untagged	L3-Untrust	
ethernet1/2	Layer3	ping-only		172.16.254.2/24	default	Untagged	L3-Intranet	
ethernet1/3	Layer3	ping-only		192.168.1.1/24	default	Untagged	L3-Trust	



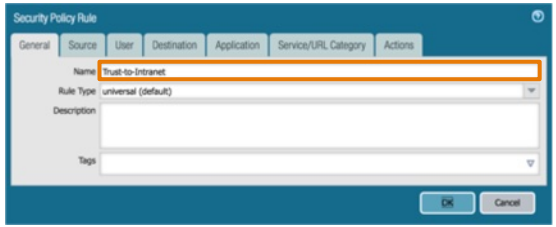
イントラネット向けルーティング設定

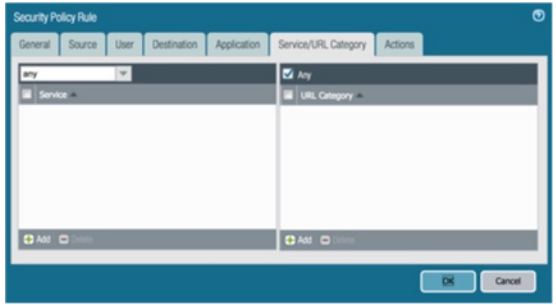
- イントラネット向けIP(デフォルト) ルート設定 (Network > Virtual Routers > default)

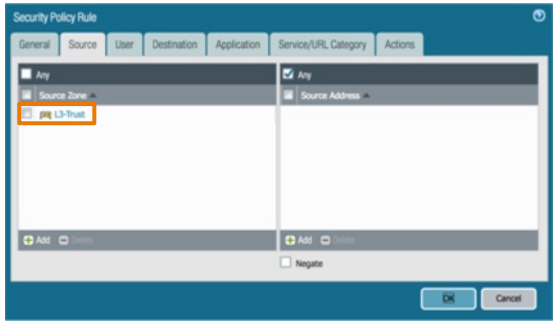


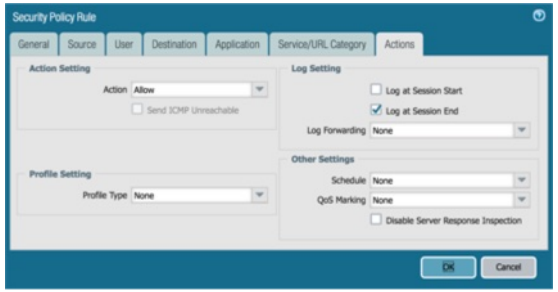
セキュリティポリシー設定

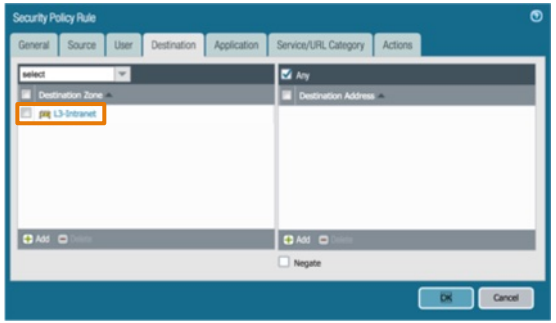
- 内部→イントラネット向け通信用セキュリティポリシーの設定 (Policies > Security > Add)





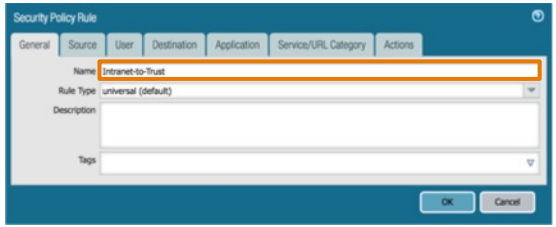


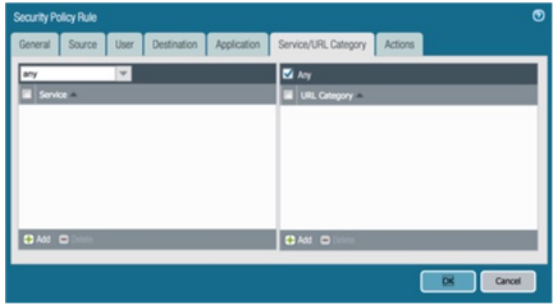


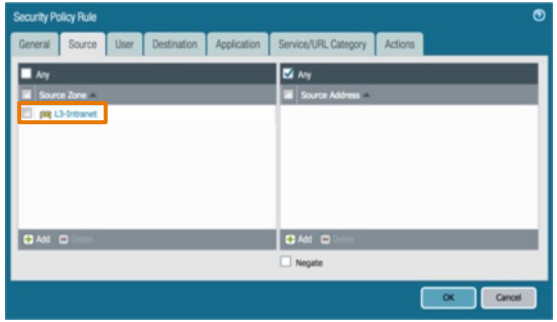


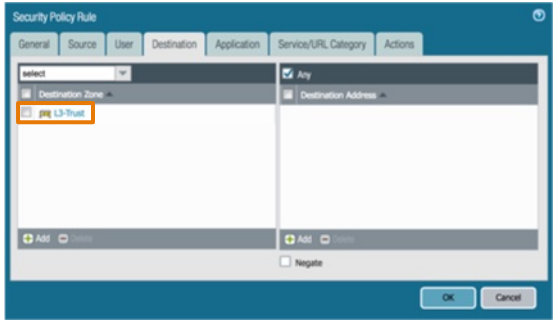
セキュリティポリシー設定

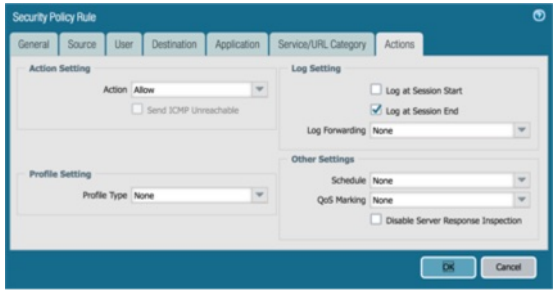
- イントラネット→内部向け通信用セキュリティポリシーの設定 (Policies > Security > Add)





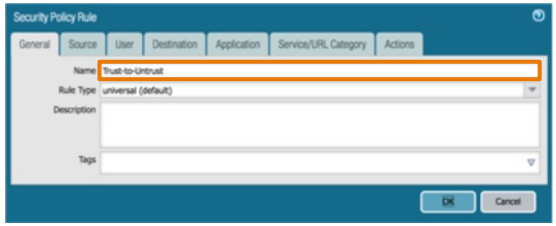


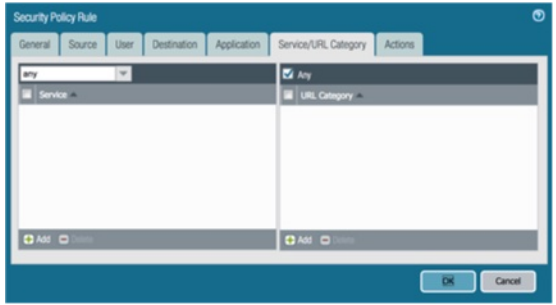


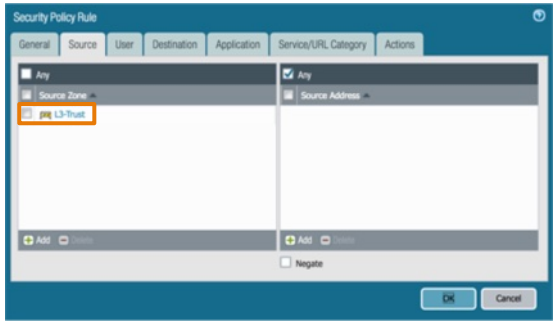


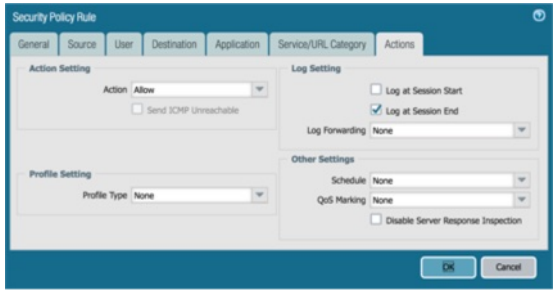
セキュリティポリシー設定

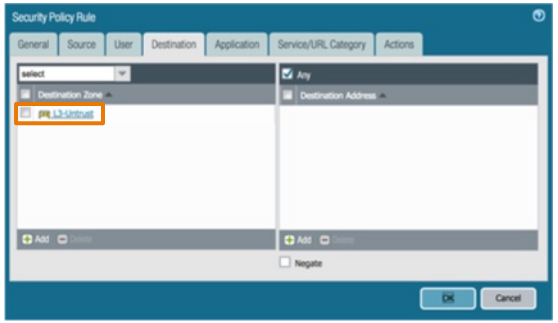
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security > Add)











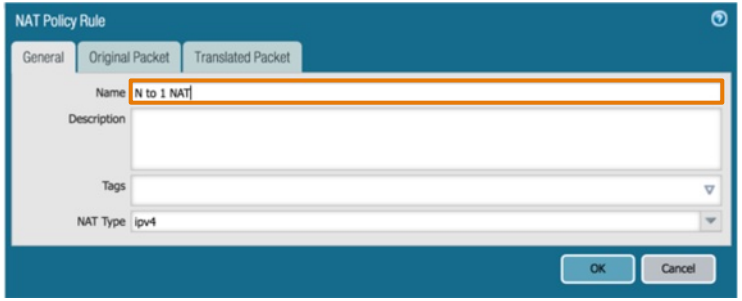
セキュリティポリシー設定一覧

- セキュリティポリシー設定一覧 (Policies > Security)

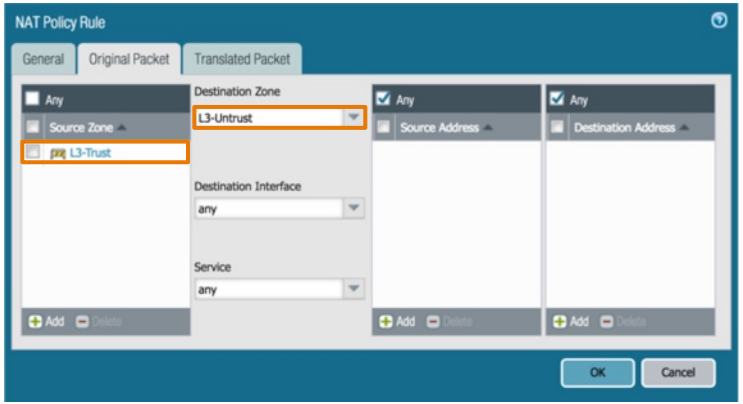
				Source			Destination						
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	Trust-to-Intranet	none	universal	L3-Trust	any	any	L3-Intranet	any	any	any	Allow	none	
2	Intranet-to-Trust	none	universal	L3-Intranet	any	any	L3-Trust	any	any	any	Allow	none	
3	Trust-to-Untrust	none	universal	L3-Trust	any	any	L3-Untrust	any	any	any	Allow	none	
4	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	none

NATポリシー設定

- インターネット向け通信用NATポリシーの設定 (Policies > NAT)



IPアドレスは指定しなくて良い
(インターフェイス に割当てられた
IPアドレスが自動的に使われる)



デフォルトルートを設定しているイントラネット向け通信については
NAT設定は行わない。
（イントラネット内のインターネット境界ファイアウォールでNAT処理を実行）

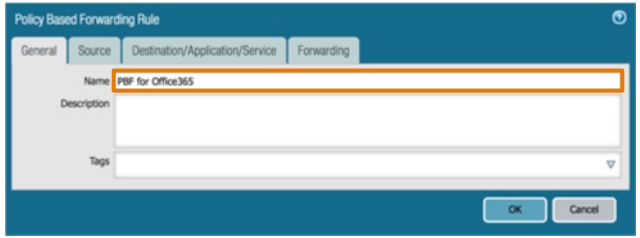
NATポリシー設定一覧

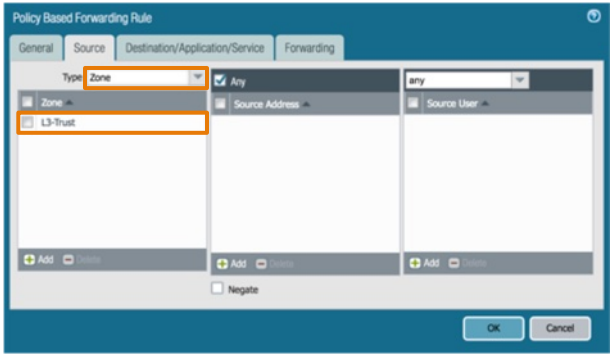
- NATポリシー設定一覧 (Policies > NAT)

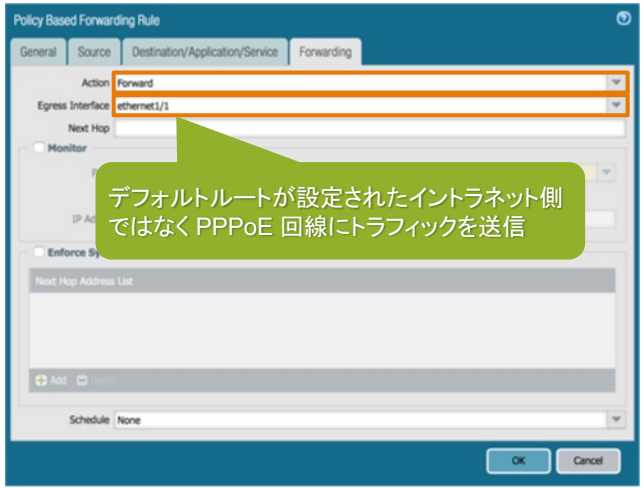
	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

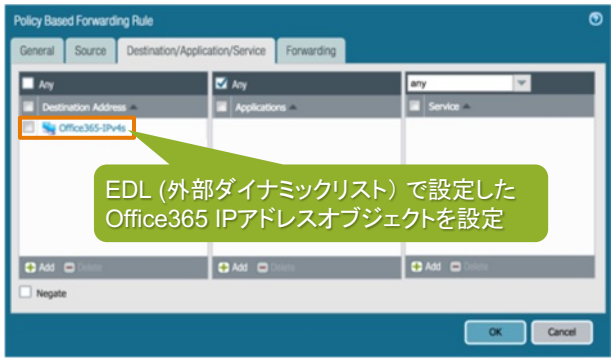
ポリシーベースフォワーディング(PBF)設定

- Office365向け通信用PBFポリシーの設定 (Policies > Policy Based Forwarding)







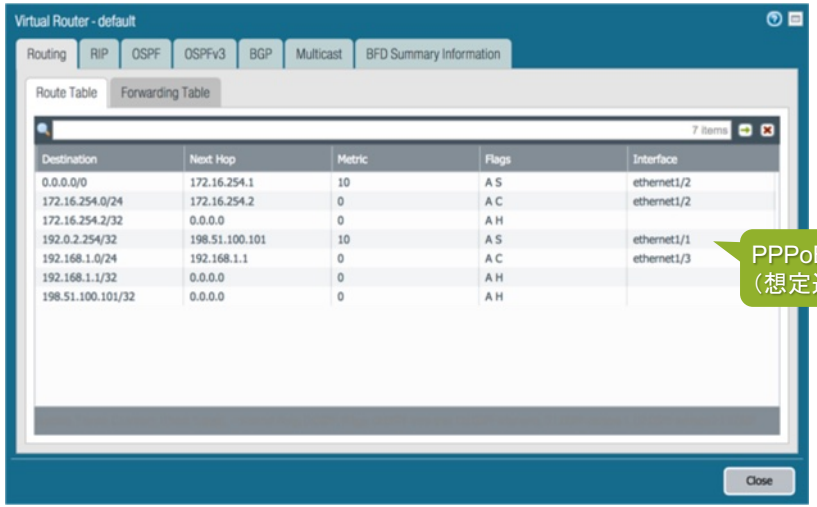


PBFポリシー設定一覧およびIP経路情報

- ポリシーベースフォワーディング設定一覧 (Policies > Policy Basaed Forwarding)

			Source			Destination				Forwarding			Monitoring			
	Name	Tags	Zone/Interface	Address	User	Address	Application	Service	Action	Egress I/F	Next Hop	Enforce Symmetric Return	Profile	Target	Disable If Unreachable	Schedule
1	PBF for Office365	none	L3-Trust	any	any	Office365-IPv4s	any	any	forward	ethernet1/1	none	false	none	none	false	none

- IP経路情報 (Network > Virtual Routers > default > More Runtime Stats)

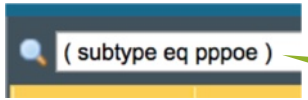


PPPoE 回線側（経由のインターネット）向けのデフォルトルートはない
（想定通りのIPルーティング情報）

設定後の**PPPoE** 接続ログ例

- PPPoE 回線接続時のログ例 (Monitor > Logs > System)

Receive Time	Type	Severity	Event	Object	Description
03/28 15:58:19	pppoe	informational	connect	ethernet1/1	PPPoE session was connected for user:dyn-ip-user101@pppoelab.local on interface:ethernet1/1 to AC:lab_pppoe_server, mac address: 00:0c:29:9f:b9:b9, session id:1, IP Address negotiated:198.51.100.101
03/28 15:58:16	pppoe	informational	initiate	ethernet1/1	PPPoE session was initiated for user:dyn-ip-user101@pppoelab.local on interface:ethernet1/1



表示フィルタを使用することで必要なログを素早く確認することが可能

EDL機能を用いて取得したOffice365 IP アドレス

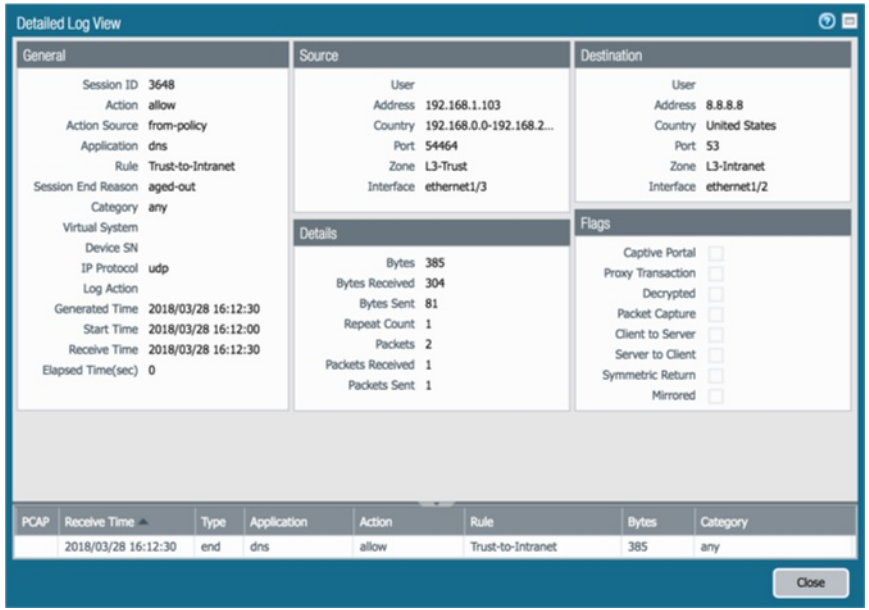
- 外部ダイナミックリスト(EDL)機能によりMineMeldから取得したOffice365 IPアドレスの確認

```
admini@PA> request system external-list show type ip name Office365-IPv4s


vsys1/Office365-IPv4s:
        Next update at       : Wed Mar 28 15:20:28 2018
        Source               : https://10.128.65.137/feeds/office365_IPv4s
        Referenced           : Yes
        Valid                : Yes

        Total valid entries   : 588
        Total invalid entries : 0
        Valid ips:
                104.208.28.54-104.208.28.54
                104.208.31.113-104.208.31.113
                104.209.188.207-104.209.188.207
                104.210.9.95-104.210.9.95
                104.41.208.54-104.41.208.54
                              .
                              .
                              .
```


設定後のトラフィックログ例

- 内部ネットワークからイントラネットを経由してインターネットへ通信した時のログ例
(Monitor > Logs > Traffic)

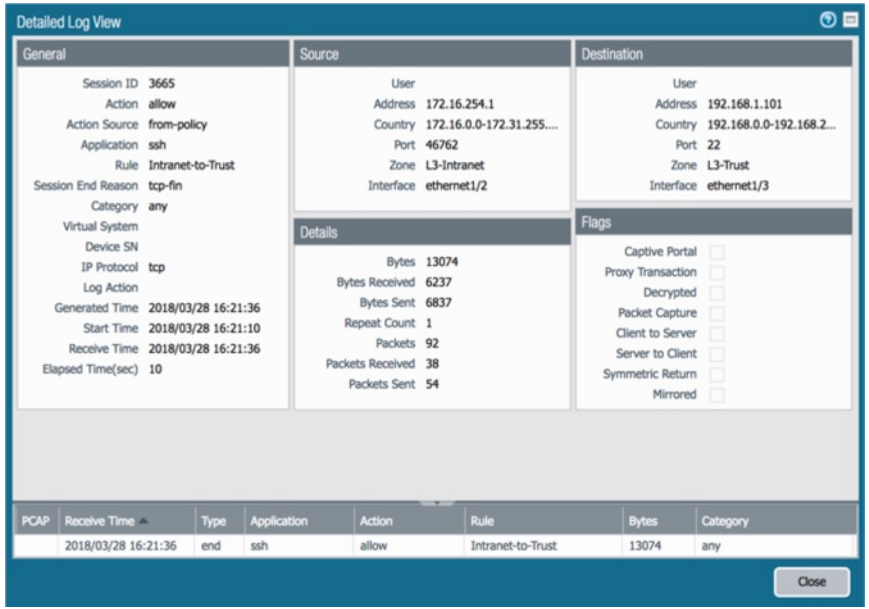
		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/28 16:12:30	end	L3-Trust	L3-Intranet	192.168.1.103	8.8.8.8	53	dns	any	allow	Trust-to-Intranet	aged-out	385



設定後のトラフィックログ例

- イントラネットから内部ネットワークへ通信した時のログ例
(Monitor > Logs > Traffic)

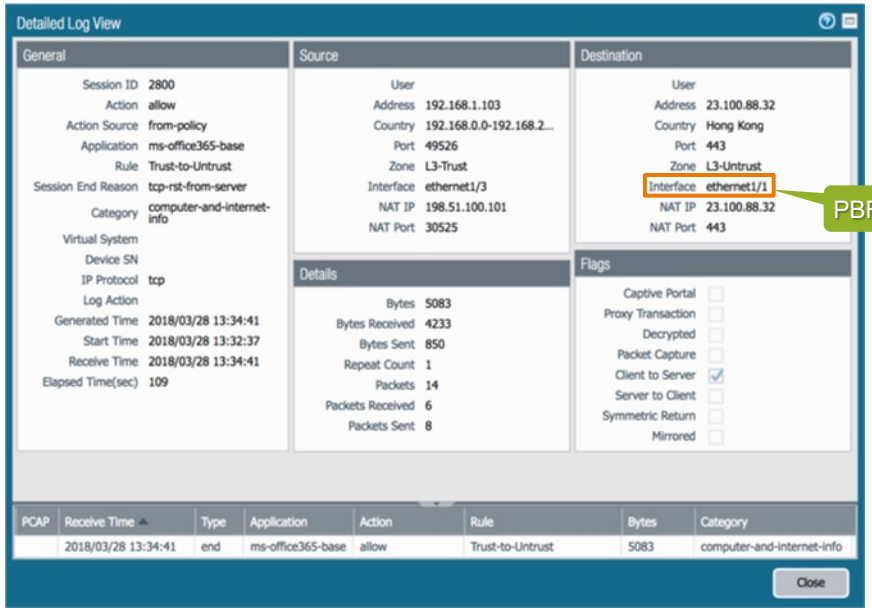
		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/28 16:21:36	end	L3-Intranet	L3-Trust	172.16.254.1	192.168.1.101	22	ssh	any	allow	Intranet-to-Trust	tcp-fin	13.1k



設定後のトラフィックログ例

- 外部ダイナミックリスト(EDL)＋ポリシーベースフォワーディング(PBF)により、PPPoE回線経由でインターネットへ直接通信した時のOffice365 トラフィックログ例 (Monitor > Logs > Traffic)

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	URL Category	Action	Rule	Session End Reason	Bytes
		03/28 13:34:41	end	L3-Trust	L3-Untrust	192.168.1.103	23.100.88.32	443	ms-office365-base	computer-and-internet-info	allow	Trust-to-Untrust	tcp-rst-from-server	5.1k



PBF設定に従って Office365 の通信がPPPoE 回線経由で行われている


paloalto
NETWORKS®