



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



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>

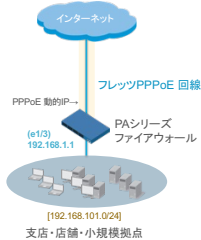
<PAN-OS 7.1関連日本語マニュアル>

<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

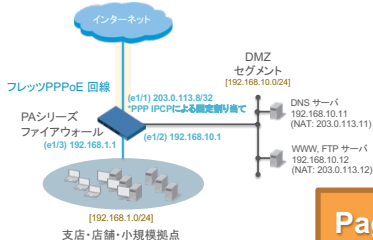
設定例 1



Page 4

最もベーシックな接続構成

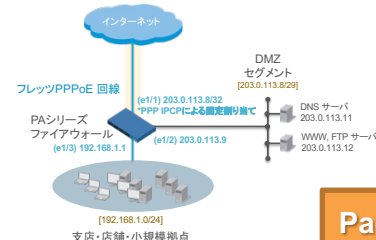
設定例 2



Page 21

公開サーバの保護1 (DMZあり構成)

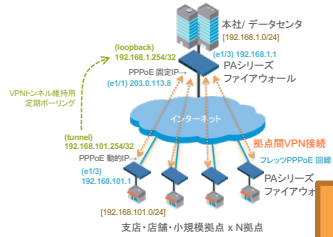
設定例 3



Page 55

公開サーバの保護2 (PPPoE Unnumbered 構成)

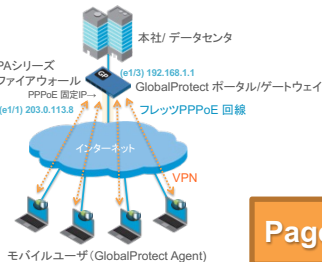
設定例 4



Page 91

拠点間 VPN 接続構成

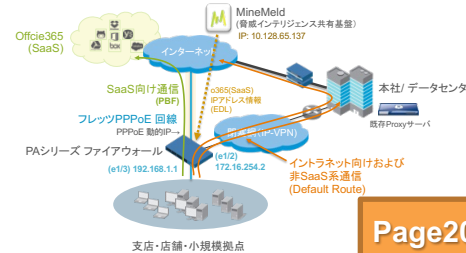
設定例 5



Page 151

GlobalProtect によるモバイル環境の保護

設定例 6



Page 209

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

設定例 1

設定例 2

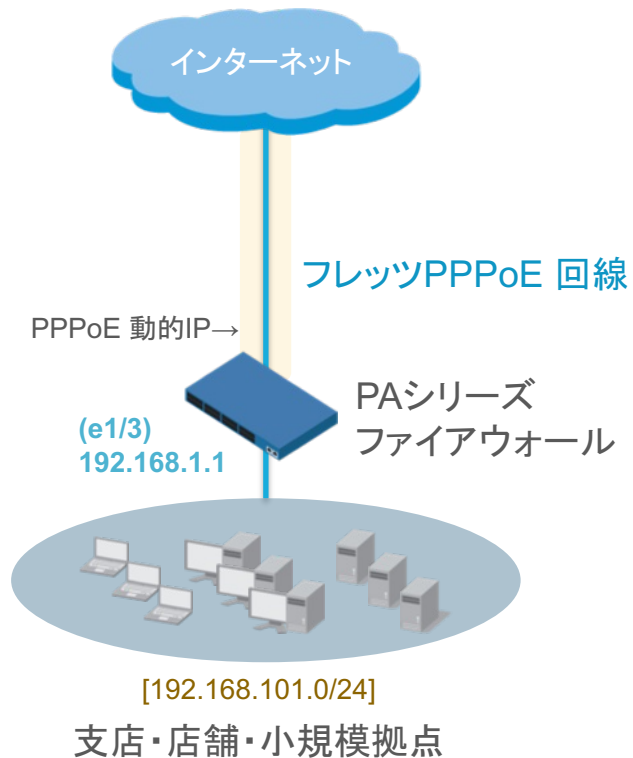
設定例 3

設定例 4

設定例 5

設定例 6

システム構成:



- 設定例 1
- 設定例 2
- 設定例 3
- 設定例 4
- 設定例 5
- 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	<ul style="list-style-type: none">・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。

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Interface Management Profile

Name

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

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)

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Trust'. The 'Name' field is 'L3-Trust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty, with 'Include List' and 'Exclude List' both showing 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24'. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Untrust'. The 'Name' field is 'L3-Untrust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty, with 'Include List' and 'Exclude List' both showing 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24'. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-Trust

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Type' is set to 'Static'. The 'IP' section contains a single entry: '192.168.1.1/24', which is highlighted with an orange box. Below the IP list are buttons for 'Add', 'Delete', 'Move Up', and 'Move Down'. The 'OK' and 'Cancel' buttons are at the bottom right.

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Type: Static PPPoE DHCP Client

IP

192.168.1.1/24

+ Add - Delete Move Up Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/3

Comment: []

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Untrust'. The 'Config' tab is active, with sub-tabs for 'IPv4' and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
Assign Interface To	
Virtual Router	default
Security Zone	L3-Untrust

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Type: Static PPPoE DHCP Client

General | Advanced

Enable

Username: dyn-ip-user101@pppaelab.local

Password: *****

Confirm Password: *****

Show PPPoE Client Runtime Info

OK Cancel

PPPoE を選択

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Type: Static PPPoE DHCP Client

General | Advanced

Authentication: auto

Static Address: None

automatically create default route pointing to peer

Default Route Metric: [1 - 65535]

Access Concentrator:

Service:

Passive

OK Cancel

PPPoE 認証方式は自動のままで良い (CHAP/PAP共にサポート)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface

OK | Cancel

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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	

Dynamic IP Interface Status

Interface ethernet1/1
Local IP Address 198.51.100.115
Primary DNS 8.8.8.8
Secondary DNS 8.8.4.4
Primary WINS 0.0.0.0
Secondary WINS 0.0.0.0
Remote IP Address 192.0.2.254
PPPoE State Connected
PPP State Connected
Access Concentrator lab_pppoe_server
AC MAC 00:0c:29:9f:b9:b9
Authentication Method CHAP
Passive mode Disabled
Link MTU 1454

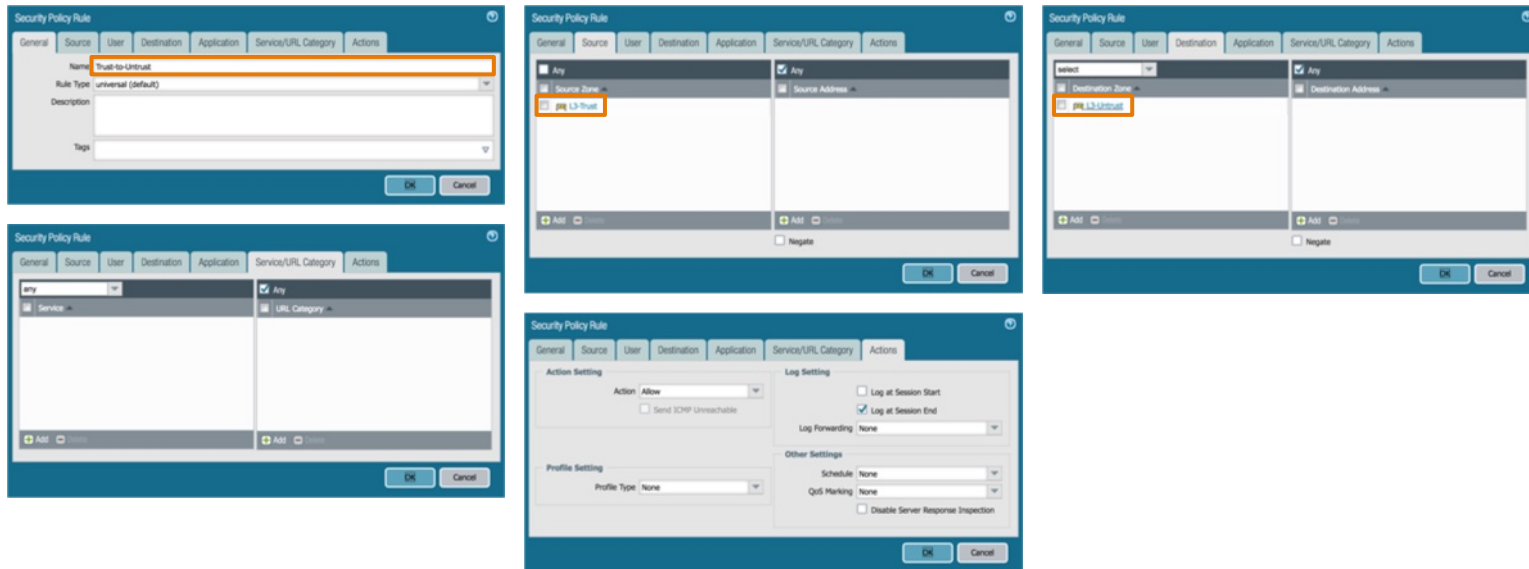
Connect Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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		intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
3	interzone-default		interzone	any	any	any	any	any	any	any	Deny	none	none

設定例 1
 設定例 2
 設定例 3
 設定例 4
 設定例 5
 設定例 6



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 Policy Rule

General Original Packet Translated Packet

Name N to 1 NAT

Description

Tags

NAT Type ipv4

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet

Source Zone L3-Trust

Destination Zone L3-Untrust

Destination Interface any

Service any

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type Dynamic IP And Port

Address Type Interface Address

Interface ethernet1/1

IP Address None

Destination Address Translation

Translated Address

Translated Port [1 - 65535]

OK Cancel

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)

Name	Tags	Original Packet				Translated Packet				
		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

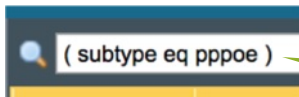
設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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

Detailed Log View

General	Source	Destination
Session ID 1805 Action allow Action Source from-policy Application facebook-base Rule Trust-to-Untrust Session End Reason tcp-rst-from-client Category social-networking Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/25 19:27:13 Start Time 2018/03/25 19:26:36 Receive Time 2018/03/25 19:27:13 Elapsed Time(sec) 22	User Address 192.168.1.102 Country 192.168.0.0-192.168.2... Port 51482 Zone L3-Trust Interface ethernet1/3 NAT IP 198.51.100.115 NAT Port 12961	User Address 157.240.15.35 Country United States Port 443 Zone L3-Untrust Interface ethernet1/1 NAT IP 157.240.15.35 NAT Port 443

Details

Bytes 9453
Bytes Received 5938
Bytes Sent 3515
Repeat Count 1
Packets 46
Packets Received 22
Packets Sent 24

Flags

Captive Portal	<input type="checkbox"/>
Proxy Transaction	<input type="checkbox"/>
Decrypted	<input type="checkbox"/>
Packet Capture	<input type="checkbox"/>
Client to Server	<input type="checkbox"/>
Server to Client	<input type="checkbox"/>
Symmetric Return	<input type="checkbox"/>
Mirrored	<input type="checkbox"/>

PCAP

Receive Time	Type	Application	Action	Rule	Bytes	Category
2018/03/25 19:27:13	end	facebook-base	allow	Trust-to-Untrust	9453	social-networking

Close

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

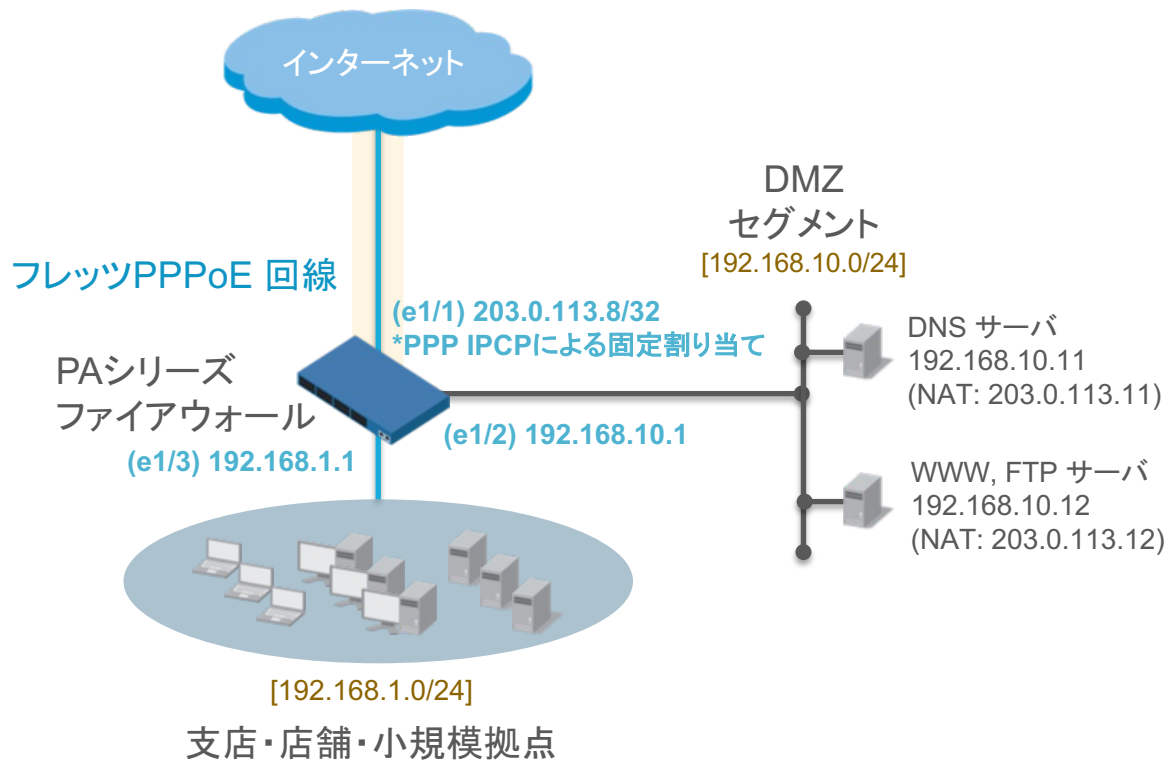
設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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	<ul style="list-style-type: none">・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)

Interface Management Profile

Name: ping-only

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

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)

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Trust'. The 'Name' field is 'L3-Trust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty, with 'Include List' and 'Exclude List' both showing 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24'. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Untrust'. The 'Name' field is 'L3-Untrust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty, with 'Include List' and 'Exclude List' both showing 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24'. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The screenshot shows the 'Zone' configuration window in Palo Alto Networks Panorama. The 'Name' field is 'L3-DMZ' and the 'Type' is 'Layer3'. The 'Zone Protection Profile' is 'None' and 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'User Identification ACL' section is visible on the right, with 'Include List' and 'Exclude List' sections. The 'Include List' section has a text input field with the placeholder 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24' and 'Add' and 'Delete' buttons. The 'Exclude List' section has a similar text input field and 'Add' and 'Delete' buttons. The 'OK' and 'Cancel' buttons are at the bottom right.

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Trust'. The 'Config' tab is active, with sub-tabs for 'IPv4', 'IPv6', and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Type' is set to 'Static'. Under the 'IP' section, the address '192.168.1.1/24' is listed and highlighted with an orange box. The 'Add', 'Delete', 'Move Up', and 'Move Down' buttons are visible at the bottom of the IP list. The 'OK' and 'Cancel' buttons are at the bottom right of the window.

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Type: Static PPPoE DHCP Client

IP

192.168.1.1/24

+ Add - Delete Move Up Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Link Settings' section shows 'Link Speed' as 'auto', 'Link Duplex' as 'auto', and 'Link State' as 'auto'. The 'Other Info' section has tabs for 'ARP Entries', 'ND Entries', 'NDP Proxy', and 'LLDP'. The 'Management Profile' dropdown menu is highlighted with an orange box and set to 'ping-only'. Below it, the 'MTU' is set to '[576 - 1500]'. There are also fields for 'Adjust TCP MSS' with 'IPv4 MSS Adjustment' set to 40 and 'IPv6 MSS Adjustment' set to 60. An 'Untagged Subinterface' checkbox is at the bottom. The 'OK' and 'Cancel' buttons are at the bottom right.

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/2'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-DMZ'. The 'Config' tab is selected, and the 'IPv4' sub-tab is active. The 'OK' and 'Cancel' buttons are at the bottom right.

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)

Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Type: Static PPPoE DHCP Client

IP
192.168.10.1/24

+ Add - Delete ↕ Move Up ↕ Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/2

Comment: []

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-Untrust

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment: [Empty]

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Type: Static PPPoE DHCP Client

General | Advanced

Enable

Username: fixed-ip-user1@pppoelab.local

Password: [Masked]

Confirm Password: [Masked]

Show PPPoE Client Runtime Info

OK Cancel

PPPoE を選択

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)

Ethernet Interface

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 Advanced

Type Static PPPoE DHCP Client

General Advanced

Authentication auto

Static Address None

automatically create default route pointing to peer

Default Route Metric [1 - 65535]

Access Concentrator

Service

Passive

OK Cancel

PPPoE 認証方式は自動のままで良い (CHAP/PAP共にサポート)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface








OK | Cancel

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	

Dynamic IP Interface Status

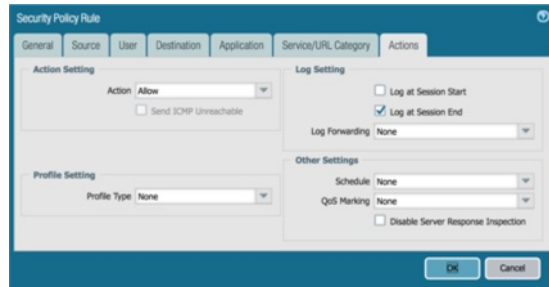
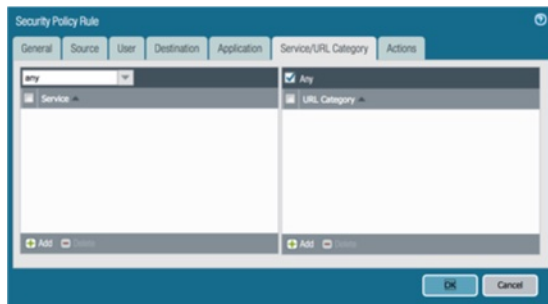
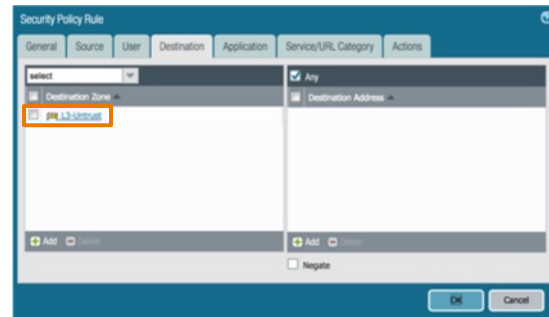
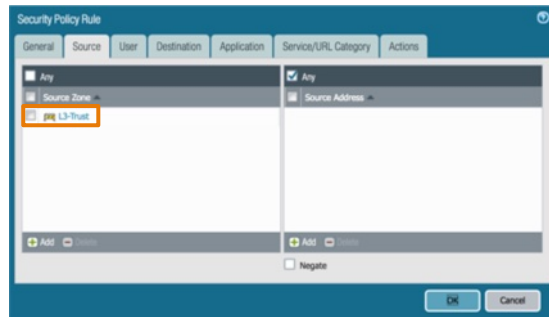
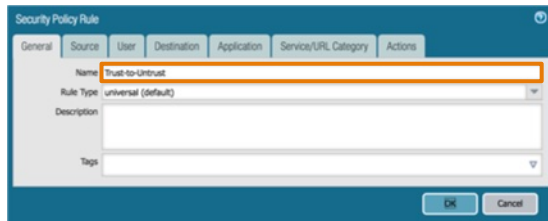
Interface ethernet1/1
Local IP Address 203.0.113.8
Primary DNS 8.8.8.8
Secondary DNS 8.8.4.4
Primary WINS 0.0.0.0
Secondary WINS 0.0.0.0
Remote IP Address 192.0.2.254
PPPoE State Connected
PPP State Connected
Access Concentrator lab_pppoe_server
AC MAC 00:0c:29:9f:b9:b9
Authentication Method CHAP
Passive mode Disabled
Link MTU 1454

Connect Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

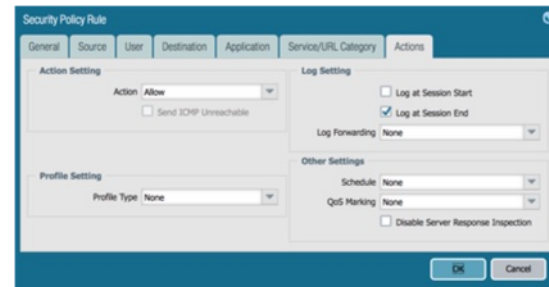
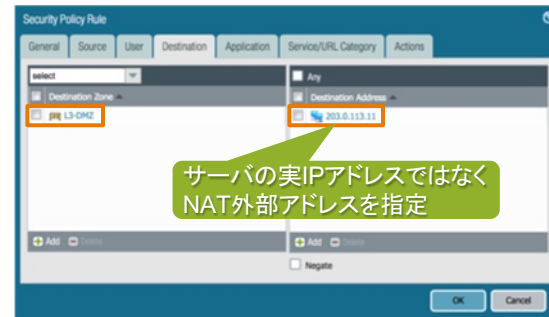
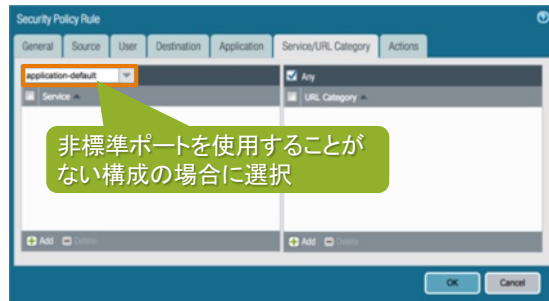
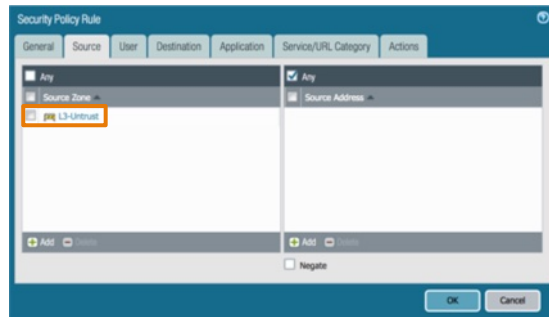
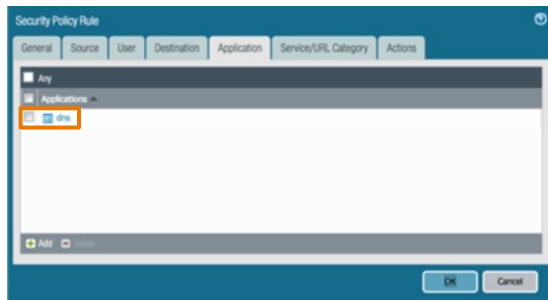
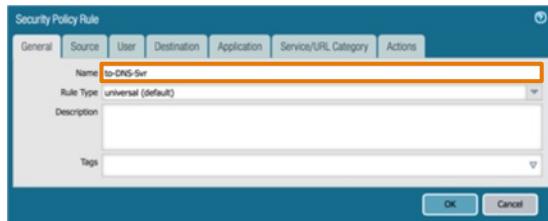
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

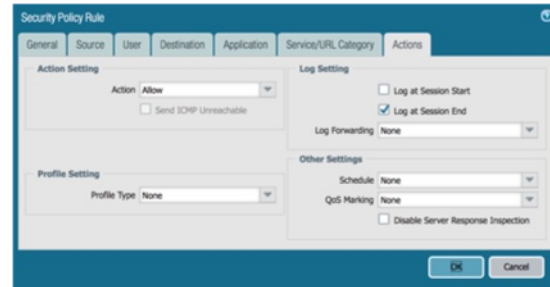
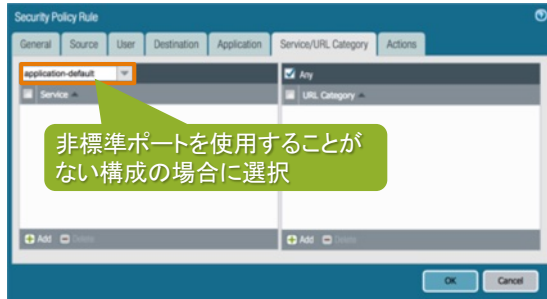
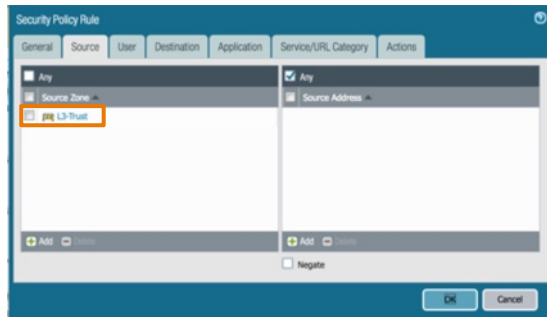
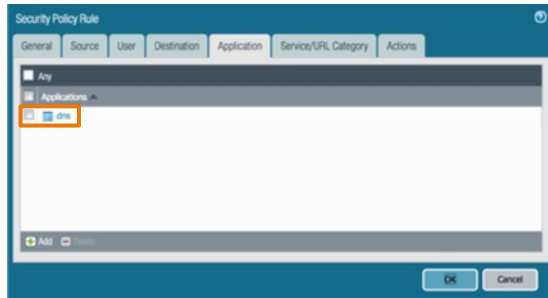
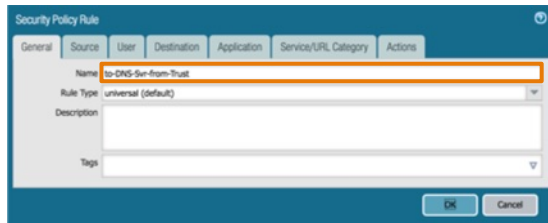
- 外部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

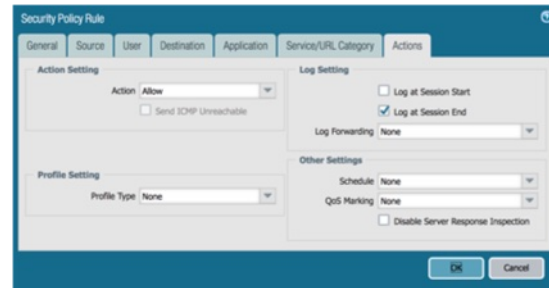
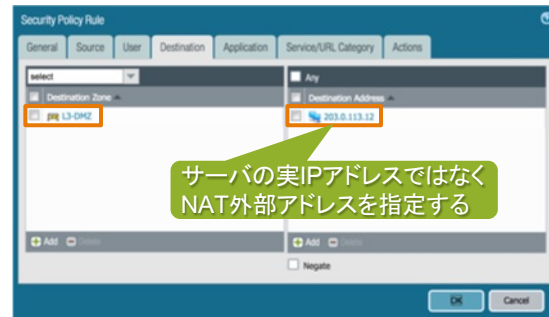
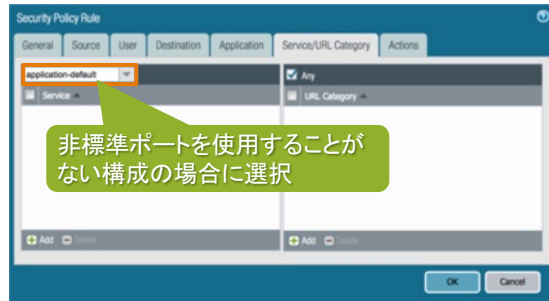
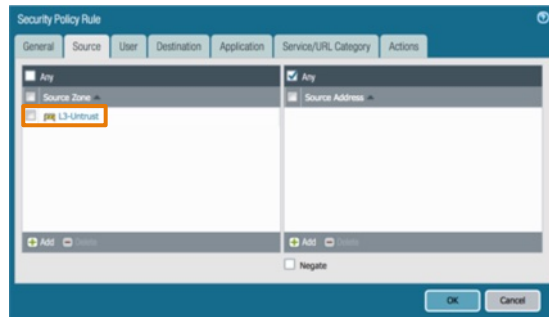
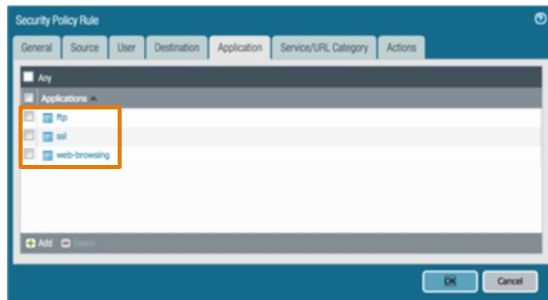
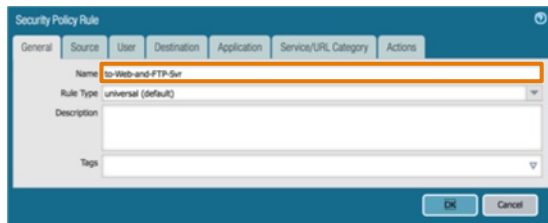
- 内部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

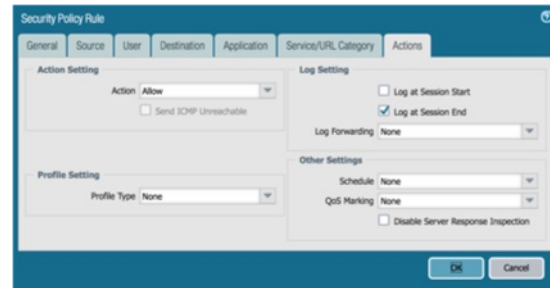
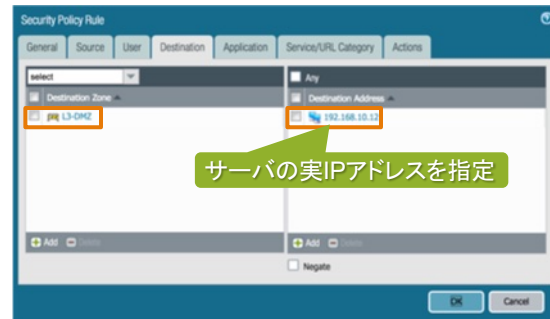
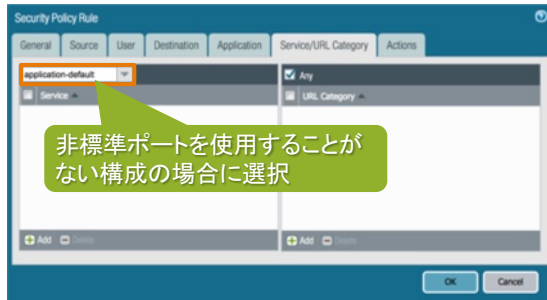
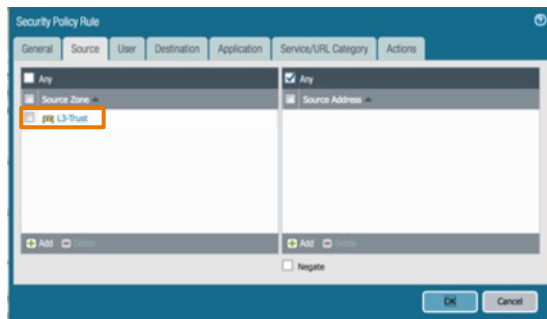
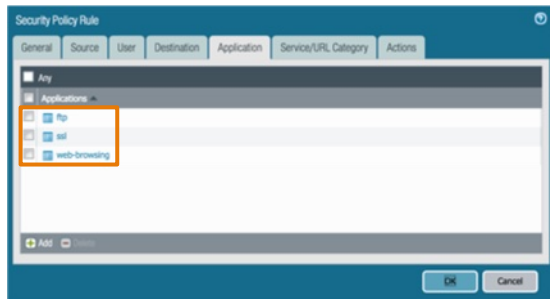
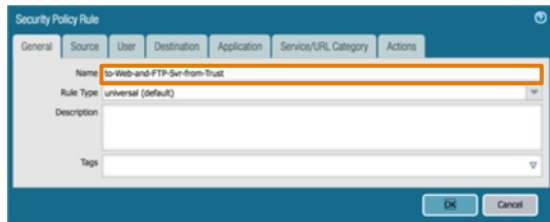
- 外部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

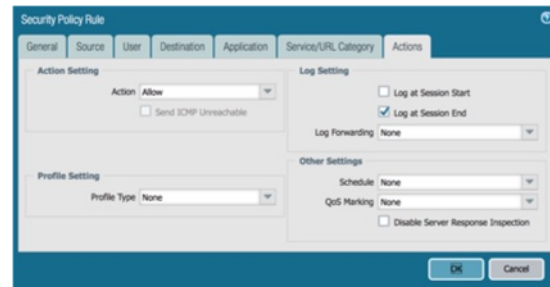
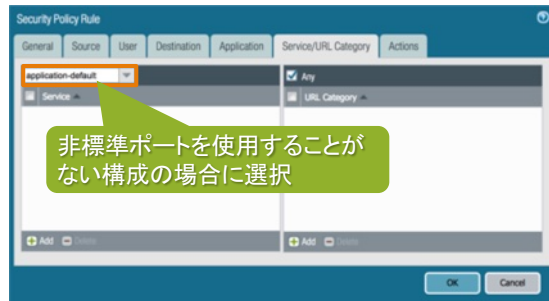
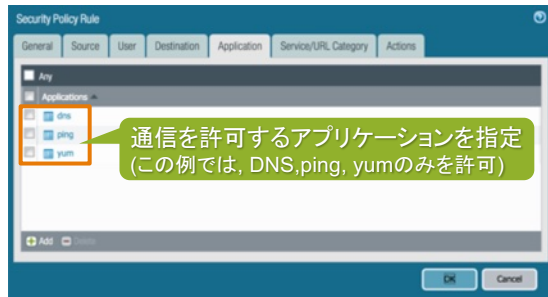
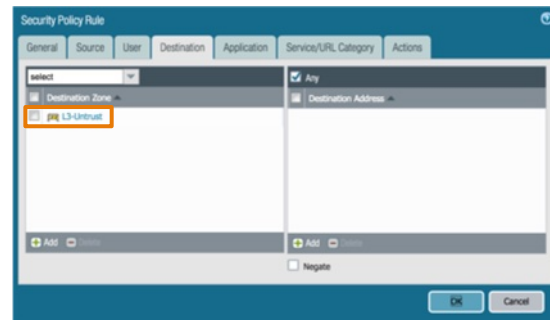
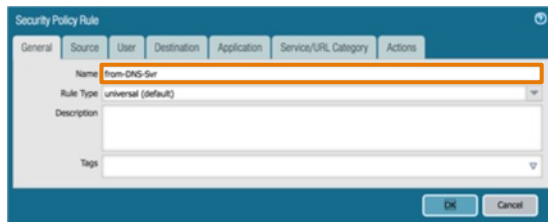
- 内部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

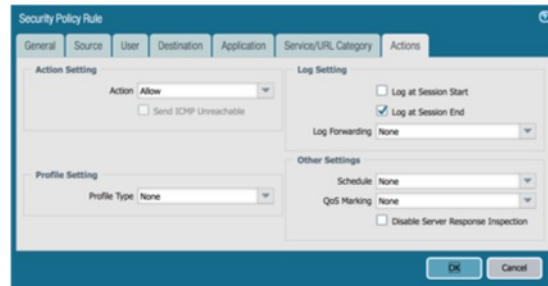
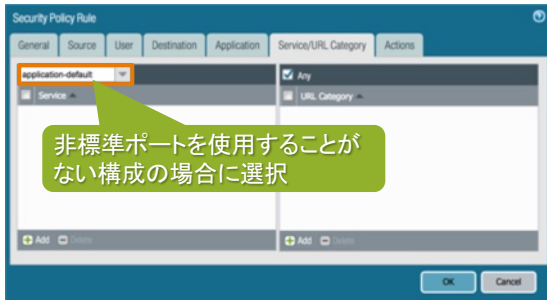
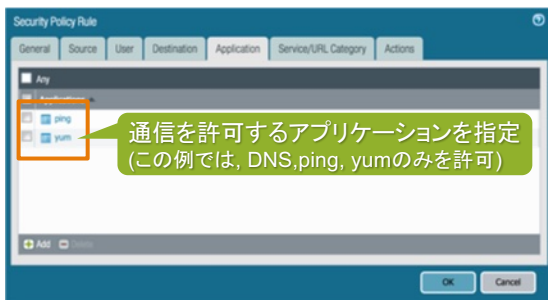
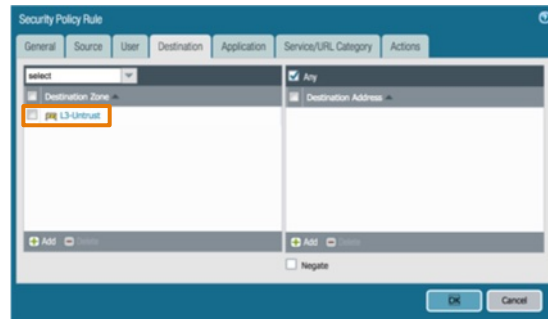
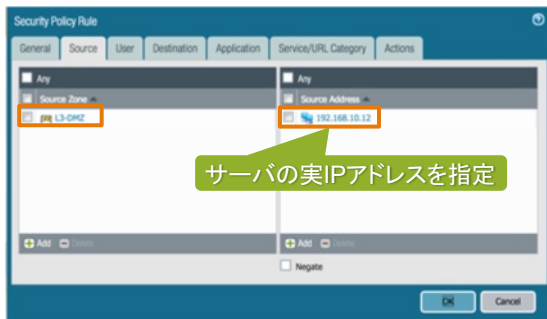
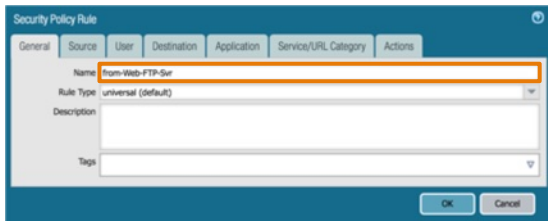
- DNSサーバ→外部向け通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)

	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	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		intrazone	any	any	any	(intrazone)	any	any	Allow	none	none	
9	interzone-default		interzone	any	any	any	any	any	any	Deny	none	none	

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Policy Rule configuration window, General tab. The Name field is set to "N to 1 NAT" and is highlighted with an orange border. The NAT Type is set to "IPv4".

NAT Policy Rule configuration window, Original Packet tab. The Destination Zone is set to "L3-Untrust" and is highlighted with an orange border. The Source Zone is set to "L3-Trust" and is also highlighted with an orange border. The Destination Interface is set to "any" and the Service is set to "any".

NAT Policy Rule configuration window, Translated Packet tab. The Source Address Translation section is active. The Translation Type is set to "Dynamic IP And Port", Address Type is "Interface Address", Interface is "ethernet1/1", and IP Address is "None". These four fields are highlighted with an orange border. The Destination Address Translation section is inactive. The Translated Address is set to "any" and the Translated Port is set to "[1 - 65535]".

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)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Policy Rule configuration window, General tab. The Name field is set to "NAT-for-DNS-Server". The NAT Type is set to "ipv4".

NAT Policy Rule configuration window, Source Address Translation tab. The Translation Type is set to "Static IP" and the Translated Address is set to "203.0.113.11". The "Bi-directional" checkbox is checked. The Destination Address Translation section is disabled.

双方向NATを有効にすることで
公開サーバのNAT設定がシンプルに

NAT Policy Rule configuration window, Translated Packet tab. The Source Zone is set to "L3-DMZ" and the Destination Zone is set to "L3-Untrust". The Source Address is set to "192.168.10.11".

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Policy Rule configuration window, General tab. The Name field is set to "NAT-for-Web-FTP-Server". The NAT Type is set to "ipv4".

NAT Policy Rule configuration window, Source Address Translation tab. The Translation Type is set to "Static IP" and the Translated Address is "203.0.113.12". The "Bi-directional" checkbox is checked. The Destination Address Translation section is disabled.

双方向NATを有効にすることで
公開サーバのNAT設定がシンプルに

NAT Policy Rule configuration window, Translated Packet tab. The Destination Zone is set to "L3-Untrust". The Source Zone is set to "L3-DMZ". The Source Address is set to "192.168.10.12".

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

NATポリシー設定一覧

- NATポリシー設定一覧 (Policies > NAT)

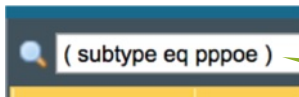
	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none
2	NAT-for-DNS-Server	L3-DMZ	L3-Untrust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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

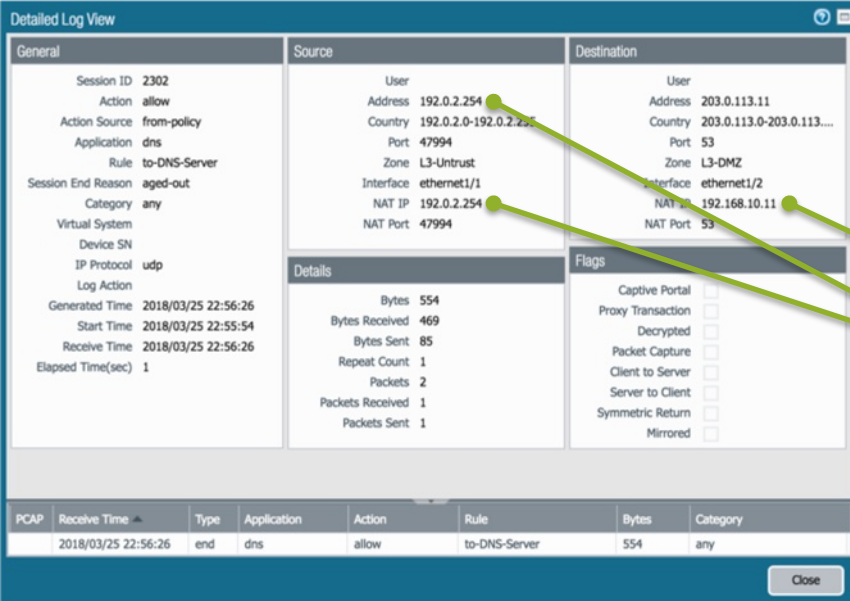


表示フィルタを使用することで必要なログを素早く確認することが可能

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



Detailed Log View

General	Source	Destination
Session ID 2302 Action allow Action Source from-policy Application dns Rule to-DNS-Server Session End Reason aged-out Category any Virtual System Device SN IP Protocol udp Log Action Generated Time 2018/03/25 22:56:26 Start Time 2018/03/25 22:55:54 Receive Time 2018/03/25 22:56:26 Elapsed Time(sec) 1	User Address 192.0.2.254 Country 192.0.2.0-192.0.2.255 Port 47994 Zone L3-Untrust Interface ethernet1/1 NAT IP 192.0.2.254 NAT Port 47994	User Address 203.0.113.11 Country 203.0.113.0-203.0.113.255 Port 53 Zone L3-DMZ Interface ethernet1/2 NAT IP 192.168.10.11 NAT Port 53

Details

Bytes 554
Bytes Received 469
Bytes Sent 85
Repeat Count 1
Packets 2
Packets Received 1
Packets Sent 1

Flags

Captive Portal <input type="checkbox"/>
Proxy Transaction <input type="checkbox"/>
Decrypted <input type="checkbox"/>
Packet Capture <input type="checkbox"/>
Client to Server <input type="checkbox"/>
Server to Client <input type="checkbox"/>
Symmetric Return <input type="checkbox"/>
Mirrored <input type="checkbox"/>

PCAP

Receive Time	Type	Application	Action	Rule	Bytes	Category
2018/03/25 22:56:26	end	dns	allow	to-DNS-Server	554	any

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 2324	User	User
Action allow	Address 192.0.2.254	Address 203.0.113.12
Action Source from-policy	Country 192.0.2.0-192.0.2.255	Country 203.0.113.0-203.0.113.255
Application web-browsing	Port 53058	Port 80
Rule to-Web-and-FTP-Server	Zone L3-Untrust	Zone L3-DMZ
Session End Reason tcp-fin	Interface ethernet1/1	Interface ethernet1/2
Category any	NAT IP 192.0.2.254	NAT IP 192.168.10.12
Virtual System	NAT Port 53058	NAT Port 80
Device SN		
IP Protocol tcp		
Log Action		
Generated Time 2018/03/25 23:01:19		
Start Time 2018/03/25 23:01:03		
Receive Time 2018/03/25 23:01:19		
Elapsed Time(sec) 1		
	Details	Flags
	Bytes 6540	Captive Portal <input type="checkbox"/>
	Bytes Received 5695	Proxy Transaction <input type="checkbox"/>
	Bytes Sent 845	Decrypted <input type="checkbox"/>
	Repeat Count 1	Packet Capture <input type="checkbox"/>
	Packets 17	Client to Server <input type="checkbox"/>
	Packets Received 8	Server to Client <input type="checkbox"/>
	Packets Sent 9	Symmetric Return <input type="checkbox"/>
		Mirrored <input type="checkbox"/>

PCAP Receive Time Type Application Action Rule Bytes Category

2018/03/25 23:01:19	end	web-browsing	allow	to-Web-and-FTP-Server	6540	any
---------------------	-----	--------------	-------	-----------------------	------	-----

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 2323 Action allow Action Source from-policy Application yum Rule from-DNS-Server Session End Reason tcp-fin Category business-and-economy Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/25 22:59:32 Start Time 2018/03/25 22:59:16 Receive Time 2018/03/25 22:59:32 Elapsed Time(sec) 0	User Address 192.168.10.11 Country 192.168.0.0-192.168.2... Port 38374 Zone L3-DMZ Interface ethernet1/2 NAT IP 203.0.113.11 NAT Port 38374	User Address 202.232.140.70 Country Japan Port 80 Zone L3-Untrust Interface ethernet1/1 NAT IP 202.232.140.70 NAT Port 80

Details

Bytes 179502
Bytes Received 174385
Bytes Sent 5117
Repeat Count 1
Packets 196
Packets Received 121
Packets Sent 75

Flags

Captive Portal	<input type="checkbox"/>
Proxy Transaction	<input type="checkbox"/>
Decrypted	<input type="checkbox"/>
Packet Capture	<input type="checkbox"/>
Client to Server	<input type="checkbox"/>
Server to Client	<input type="checkbox"/>
Symmetric Return	<input type="checkbox"/>
Mirrored	<input type="checkbox"/>

送信元 IPアドレスが Static NAT 外部 IPアドレスに変換される

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/25 22:59:32	end	yum	allow	from-DNS-Server	179502	business-and-economy

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 2433 Action allow Action Source from-policy Application dns Rule to-DNS-Svr-from-Trust Session End Reason aged-out Category any Virtual System Device SN IP Protocol udp Log Action Generated Time 2018/03/26 00:56:50 Start Time 2018/03/26 00:56:19 Receive Time 2018/03/26 00:56:50 Elapsed Time(sec) 1	User Address 192.168.1.102 Country 192.168.0.0-192.168.2... Port 42422 Zone L3-Trust Interface ethernet1/3	User Address 192.168.10.11 Country 192.168.0.0-192.168.2... Port 53 Zone L3-DMZ Interface ethernet1/2
	Details	Flags
	Bytes 237 Bytes Received 166 Bytes Sent 71 Repeat Count 1 Packets 2 Packets Received 1 Packets Sent 1	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/26 00:56:50	end	dns	allow	to-DNS-Svr-from-Trust	237	any

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

設定例 1

設定例 2

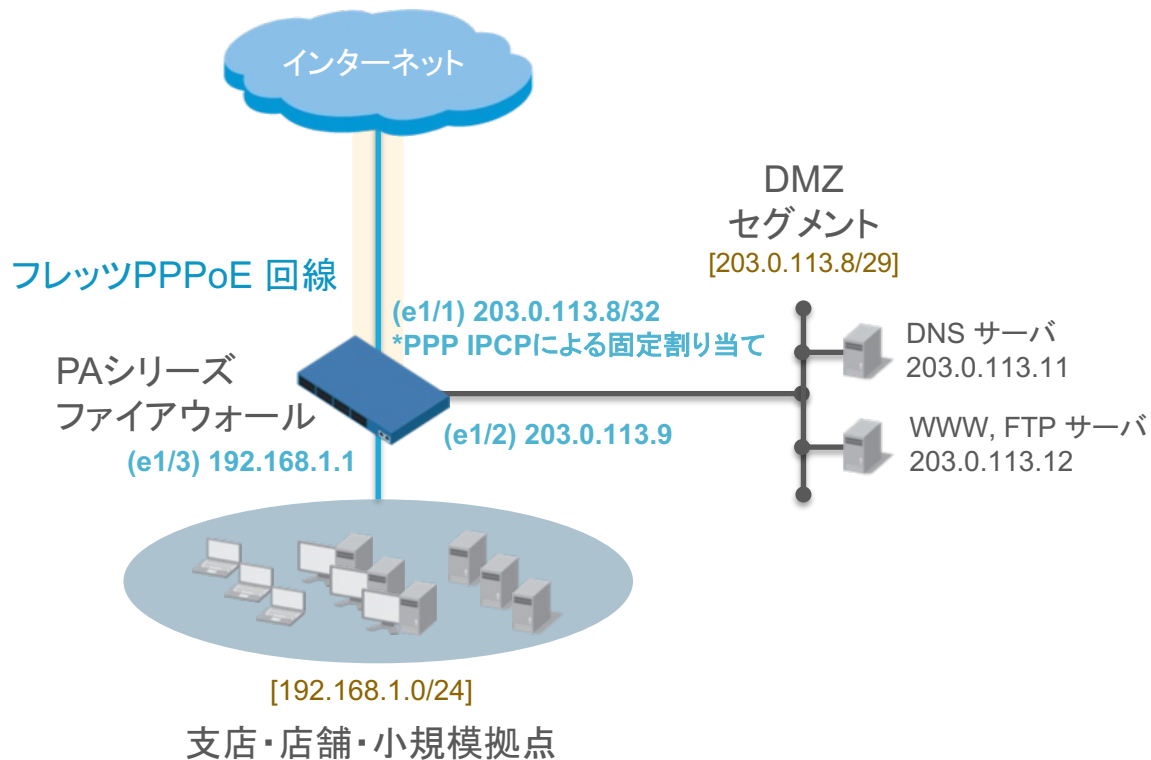
設定例 3

設定例 4

設定例 5

設定例 6

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	<ul style="list-style-type: none">・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	<ul style="list-style-type: none">・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)

Interface Management Profile

Name

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Trust'. The 'Name' field is 'L3-Trust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Untrust'. The 'Name' field is 'L3-Untrust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

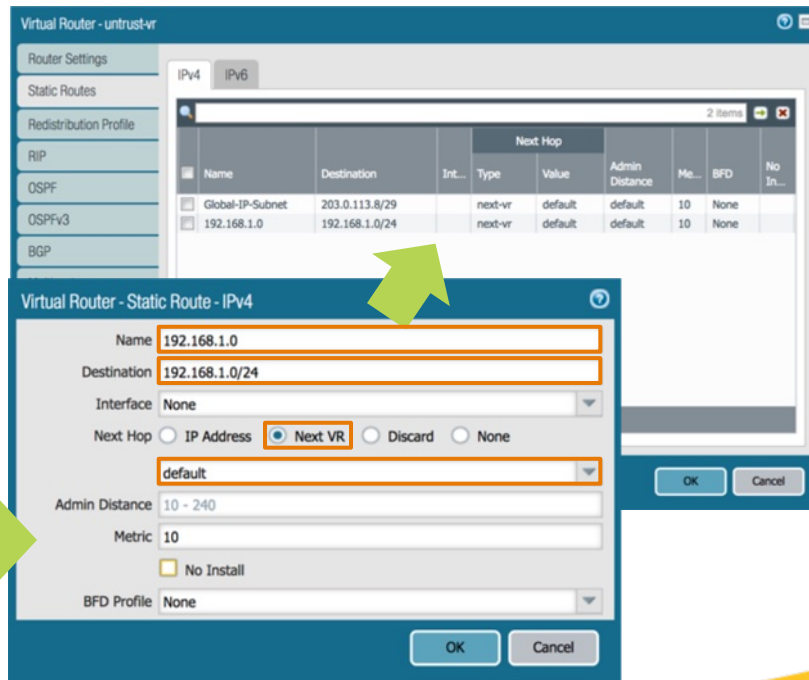
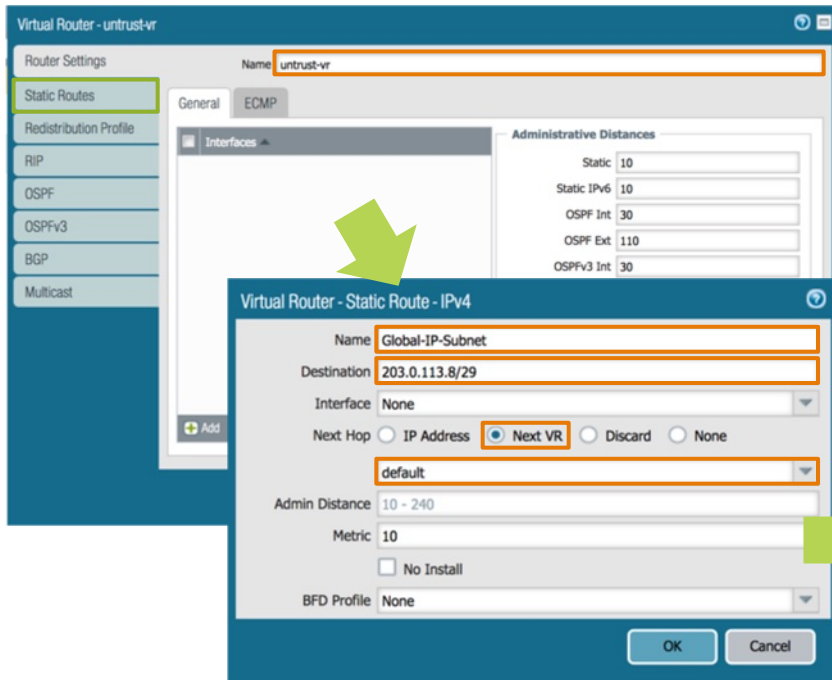
セキュリティゾーン設定

- 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)

The screenshot shows the 'Zone' configuration window in Palo Alto Networks Panorama. The 'Name' field is 'L3-DMZ' and the 'Type' is 'Layer3'. The 'Zone Protection Profile' is set to 'None' and 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'User Identification ACL' section is visible on the right, with 'Include List' and 'Exclude List' sections. The 'Include List' section has a text input field with the placeholder 'Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24' and 'Add' and 'Delete' buttons. The 'Exclude List' section has a similar text input field and 'Add' and 'Delete' buttons. The 'OK' and 'Cancel' buttons are at the bottom right.

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)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The image displays three overlapping screenshots from the Palo Alto Networks configuration interface, illustrating the steps to add a static route to a virtual router.

Left Screenshot: Virtual Router - default
The "Static Routes" tab is selected. The "Name" field is set to "default". The "Administrative Distances" section shows values for Static (10), Static IPv6 (10), OSPF Int (30), OSPF Ext (110), and OSPFv3 Int (30).

Right Screenshot: Virtual Router - default
The "Static Routes" table shows one entry:

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	No Install
default	0.0.0.0/0		next-vr	untrust-vr	default	10	None	

Center Screenshot: Virtual Router - Static Route - IPv4
This dialog box shows the configuration for the static route:

- Name: default
- Destination: 0.0.0.0/0
- Interface: None
- Next Hop: Next VR
- Next Hop Value: untrust-vr
- Admin Distance: 10 - 240
- Metric: 10
- No Install
- BFD Profile: None

Green arrows indicate the flow of information from the left screenshot to the center dialog, and from the center dialog to the right screenshot.

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. Below these fields are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced'. The 'Assign Interface To' section contains two dropdown menus: 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Trust'. 'OK' and 'Cancel' buttons are at the bottom right.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Type' is set to 'Static'. The 'IP' section contains a single entry '192.168.1.1/24', which is highlighted with an orange box. The 'Add', 'Delete', 'Move Up', and 'Move Down' buttons are visible at the bottom of the IP list. The 'OK' and 'Cancel' buttons are at the bottom right of the window.

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Type: Static PPPoE DHCP Client

IP

192.168.1.1/24

+ Add - Delete Move Up Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/3

Comment: []

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/2'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-DMZ'. The 'Config' tab is active, with sub-tabs for 'IPv4', 'IPv6', and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Type: Static PPPoE DHCP Client

IP

203.0.113.9/29

グローバル IPアドレスを設定

Add Delete Move Up Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/2

Comment: []

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

設定例1
設定例2
設定例3
設定例4
設定例5
設定例6



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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Assign Interface To

Virtual Router: untrust-vr

Security Zone: L3-Untrust

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | **Advanced**

Type: Static **PPPoE** DHCP Client

General | **Advanced**

Enable

Username: fixed-ip-user1@pppoelab.local

Password: *****

Confirm Password: *****

Show PPPoE Client Runtime Info

OK Cancel

PPPoE を選択

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 Advanced

Type Static PPPoE DHCP Client

General Advanced

Authentication auto

Static Address None

automatically create default route pointing to peer

Default Route Metric [1 - 65535]

Access Concentrator

Service

Passive

OK Cancel

PPPoE 認証方式は自動のままで良い (CHAP/PAP共にサポート)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface

OK Cancel








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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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	

Dynamic IP Interface Status

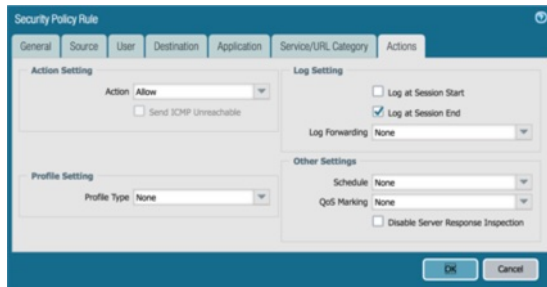
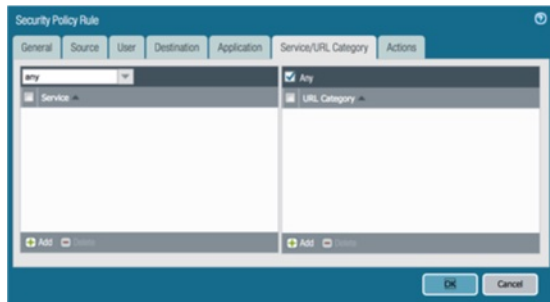
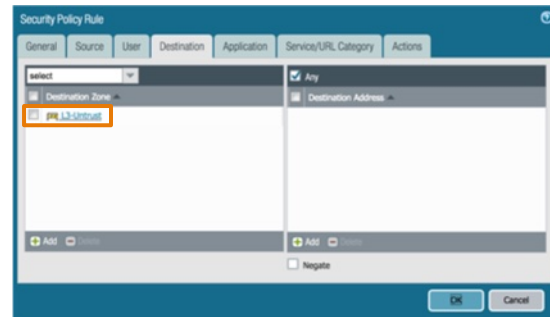
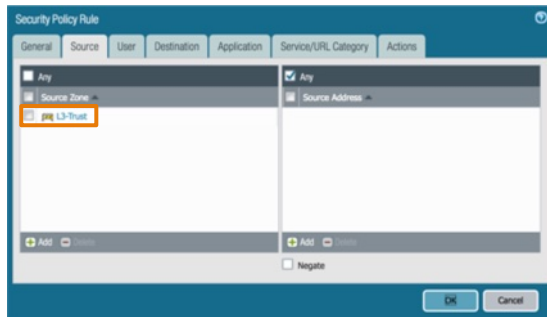
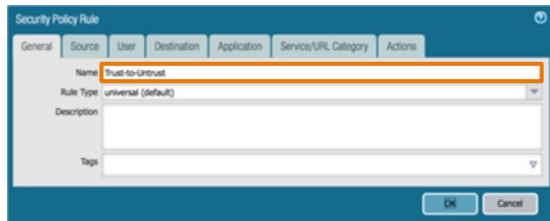
Interface ethernet1/1
Local IP Address 203.0.113.8
Primary DNS 8.8.8.8
Secondary DNS 8.8.4.4
Primary WINS 0.0.0.0
Secondary WINS 0.0.0.0
Remote IP Address 192.0.2.254
PPPoE State Connected
PPP State Connected
Access Concentrator lab_pppoe_server
AC MAC 00:0c:29:9f:b9:b9
Authentication Method CHAP
Passive mode Disabled
Link MTU 1454

Connect Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

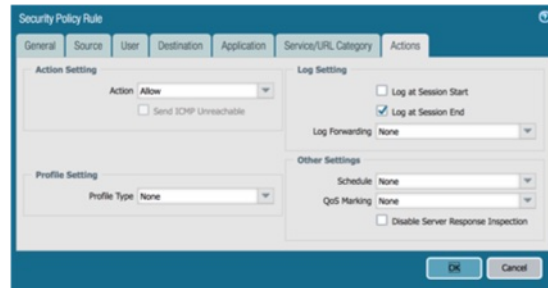
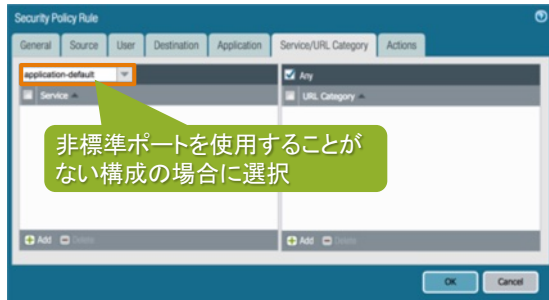
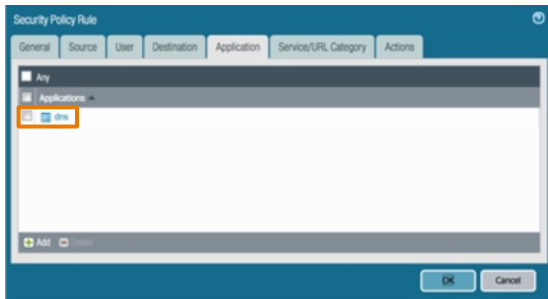
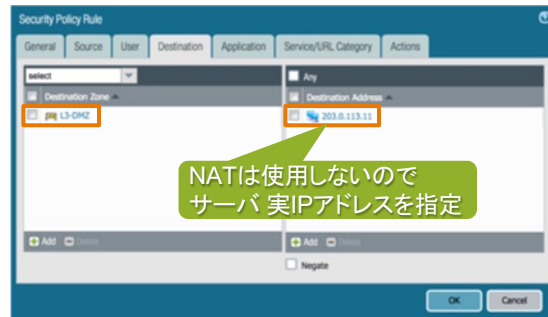
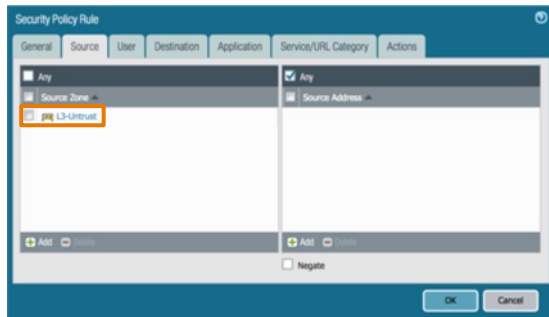
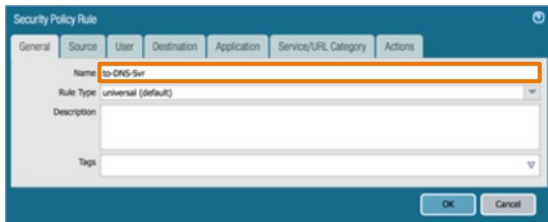
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

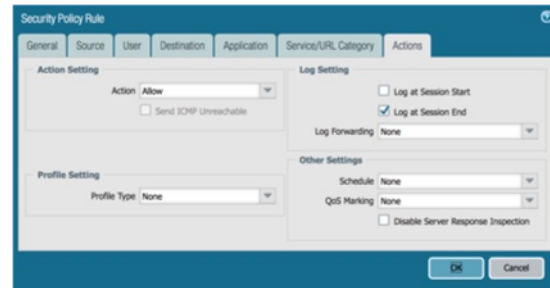
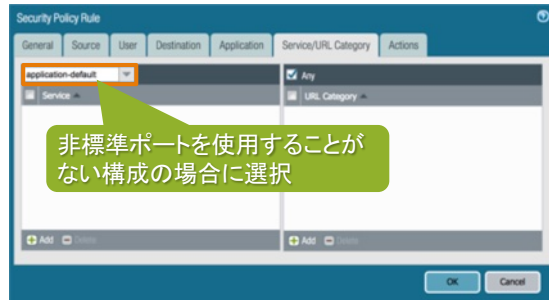
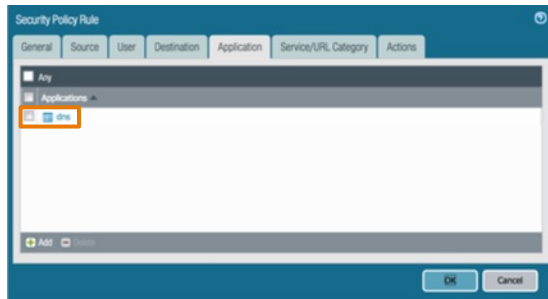
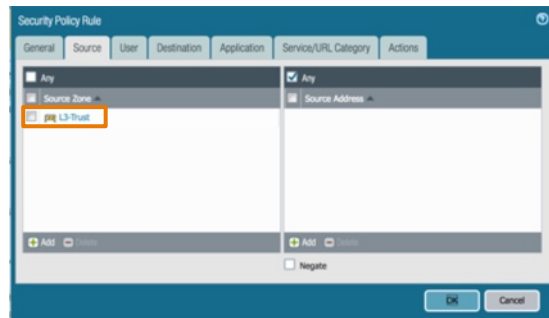
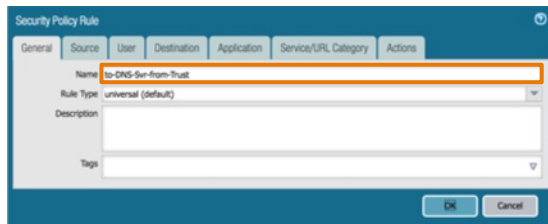
- 外部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

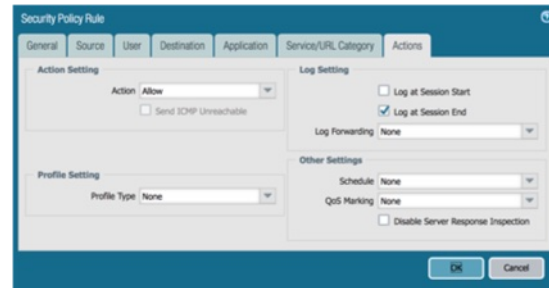
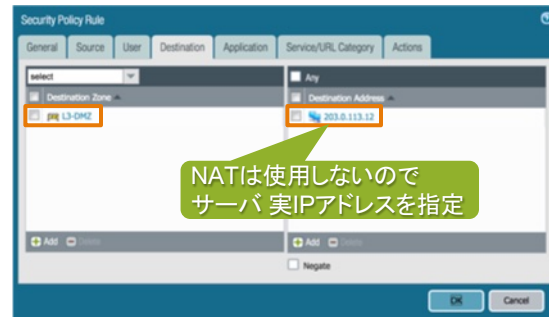
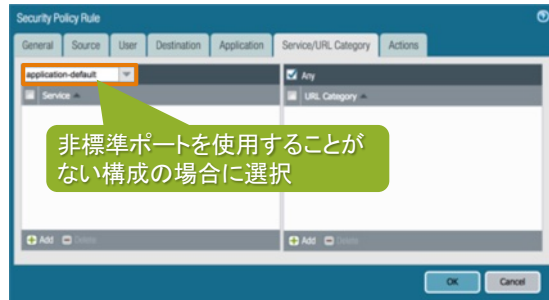
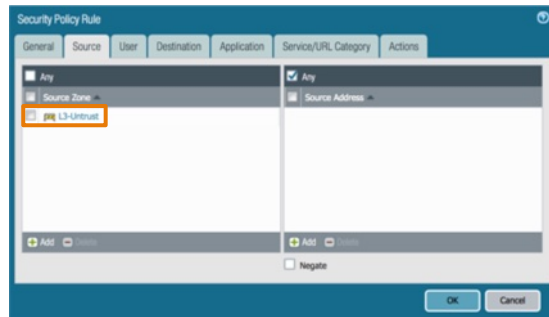
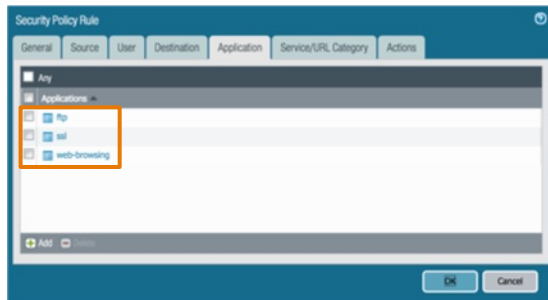
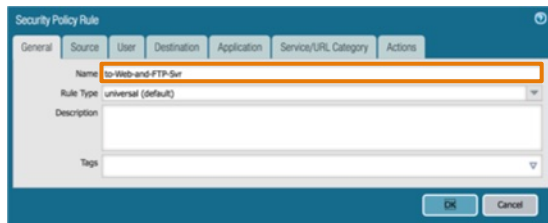
- 内部→DMZサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

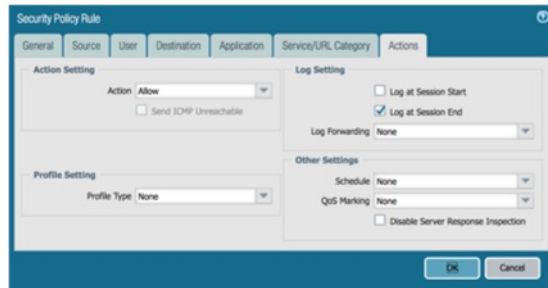
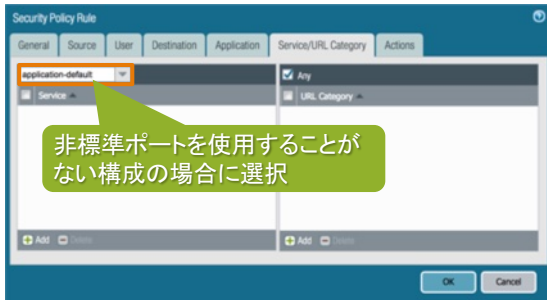
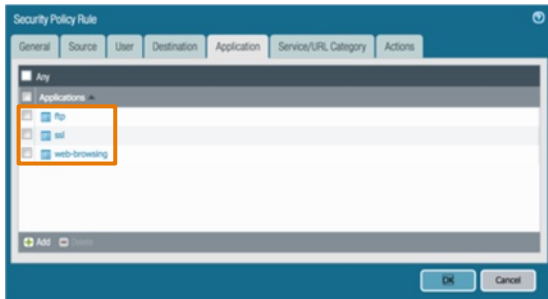
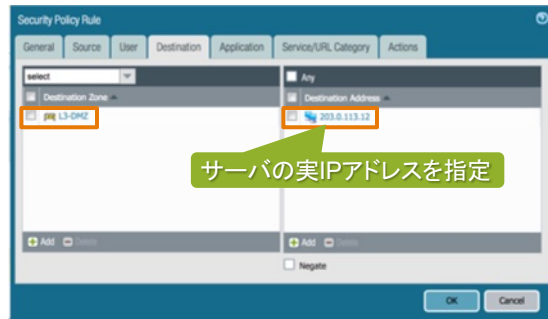
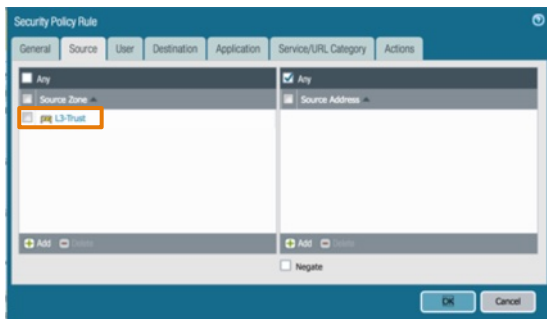
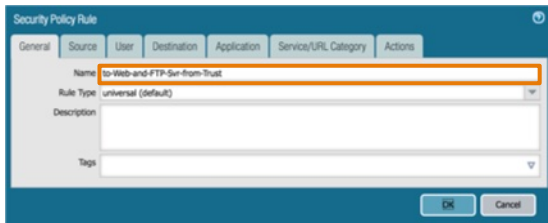
- 外部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

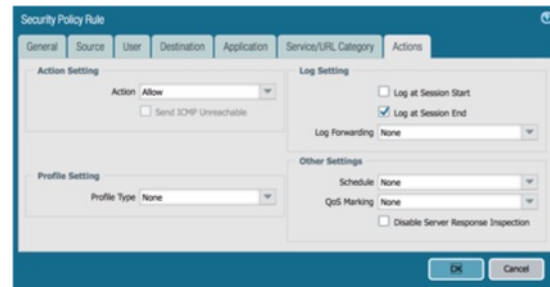
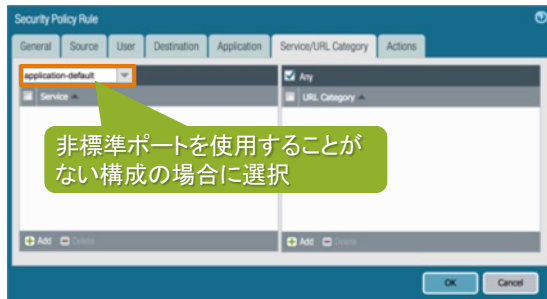
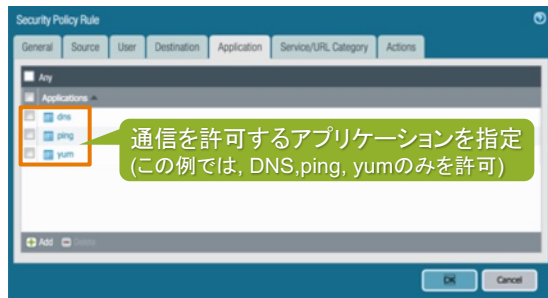
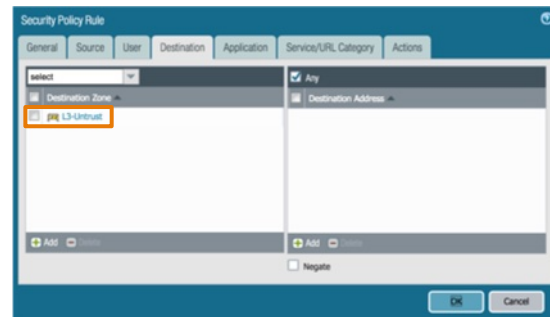
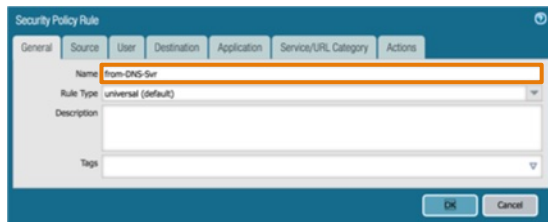
- 内部→Web/FTPサーバ向けDNS通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

セキュリティポリシー設定

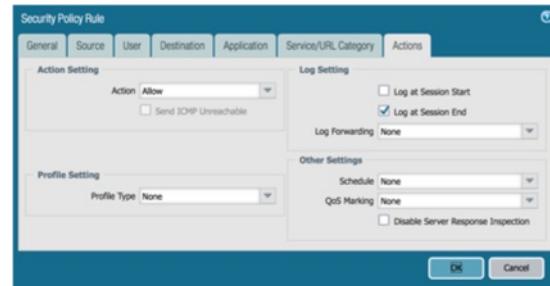
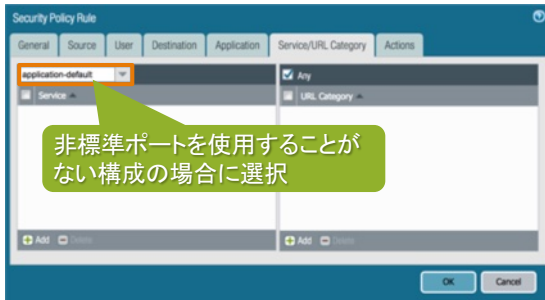
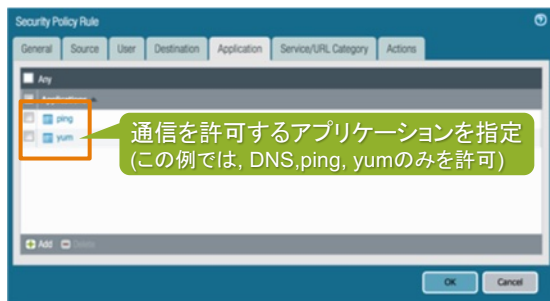
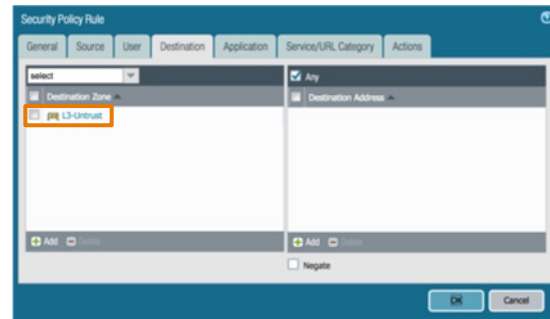
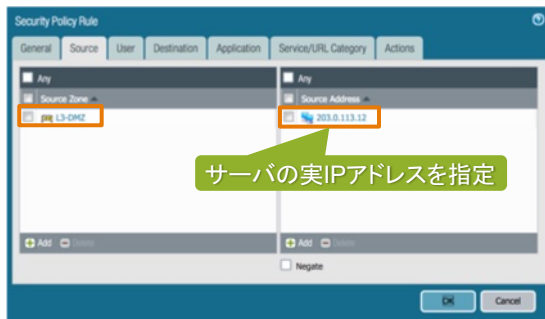
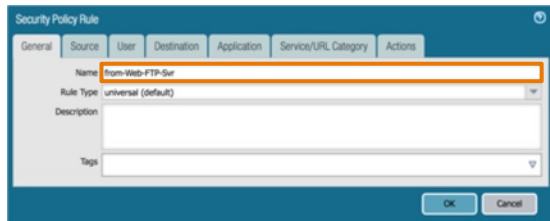
- DNSサーバ→外部向け通信用セキュリティポリシーの設定 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)

	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	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		intrazone	any	any	any	(intrazone)	any	any	Allow	none	none	
9	interzone-default		interzone	any	any	any	any	any	any	Deny	none	none	

設定例 1

設定例 2

設定例 3

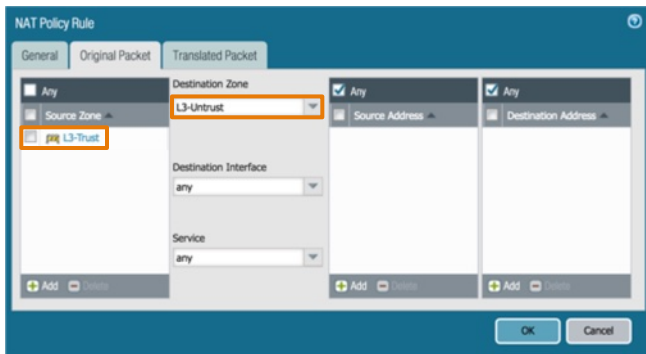
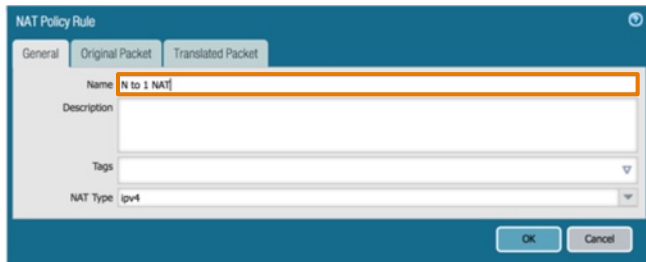
設定例 4

設定例 5

設定例 6

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)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

NATポリシー設定一覧

- NATポリシー設定一覧 (Policies > NAT)

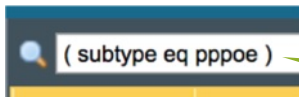
	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	 L3-Trust	 L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 4095 Action allow Action Source from-policy Application dns Rule to-DNS-Svr Session End Reason aged-out Category any Virtual System Device SN IP Protocol udp Log Action Generated Time 2018/03/26 07:33:29 Start Time 2018/03/26 07:32:58 Receive Time 2018/03/26 07:33:29 Elapsed Time(sec) 0	User Address 192.0.2.254 Country 192.0.2.0-192.0.2.255 Port 33546 Zone L3-Untrust Interface ethernet1/1	User Address 203.0.113.11 Country 203.0.113.0-203.0.113.255 Port 53 Zone L3-DMZ Interface ethernet1/2

Details

Bytes 412
Bytes Received 334
Bytes Sent 78
Repeat Count 1
Packets 2
Packets Received 1
Packets Sent 1

Flags

Captive Portal <input type="checkbox"/>
Proxy Transaction <input type="checkbox"/>
Decrypted <input type="checkbox"/>
Packet Capture <input type="checkbox"/>
Client to Server <input type="checkbox"/>
Server to Client <input type="checkbox"/>
Symmetric Return <input type="checkbox"/>
Mirrored <input type="checkbox"/>

PCAP

Receive Time	Type	Application	Action	Rule	Bytes	Category
2018/03/26 07:33:29	end	dns	allow	to-DNS-Svr	412	any

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 4096 Action allow Action Source from-policy Application web-browsing Rule to-Web-and-FTP-Svr Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/26 07:33:14 Start Time 2018/03/26 07:32:58 Receive Time 2018/03/26 07:33:14 Elapsed Time(sec) 0	User Address 192.0.2.254 Country 192.0.2.0-192.0.2.255 Port 47836 Zone L3-Untrust Interface ethernet1/1	User Address 203.0.113.12 Country 203.0.113.0-203.0.113.255 Port 80 Zone L3-DMZ Interface ethernet1/2

Details

Bytes 6458
Bytes Received 5695
Bytes Sent 763
Repeat Count 1
Packets 16
Packets Received 8
Packets Sent 8

Flags

Captive Portal <input type="checkbox"/>
Proxy Transaction <input type="checkbox"/>
Decrypted <input type="checkbox"/>
Packet Capture <input type="checkbox"/>
Client to Server <input type="checkbox"/>
Server to Client <input type="checkbox"/>
Symmetric Return <input type="checkbox"/>
Mirrored <input type="checkbox"/>

PCAP

Receive Time	Type	Application	Action	Rule	Bytes	Category
2018/03/26 07:33:14	end	web-browsing	allow	to-Web-and-FTP-Svr	6458	any

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 4579 Action allow Action Source from-policy Application yum Rule from-DNS-Svr Session End Reason tcp-fin Category business-and-economy Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/26 08:11:12 Start Time 2018/03/26 08:10:57 Receive Time 2018/03/26 08:11:12 Elapsed Time(sec) 0	User Address 203.0.113.11 Country 203.0.113.0-203.0.113... Port 41122 Zone L3-DMZ Interface ethernet1/2	User Address 202.232.140.70 Country Japan Port 80 Zone L3-Untrust Interface ethernet1/1
	Details	Flags
	Bytes 4811 Bytes Received 4196 Bytes Sent 615 Repeat Count 1 Packets 14 Packets Received 7 Packets Sent 7	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP

Receive Time	Type	Application	Action	Rule	Bytes	Category
2018/03/26 08:11:12	end	yum	allow	from-DNS-Svr	4811	business-and-economy

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 4104 Action allow Action Source from-policy Application dns Rule to-DNS-Svr-from-Trust Session End Reason aged-out Category any Virtual System Device SN IP Protocol udp Log Action Generated Time 2018/03/26 07:33:42 Start Time 2018/03/26 07:33:11 Receive Time 2018/03/26 07:33:42 Elapsed Time(sec) 0	User Address 192.168.1.102 Country 192.168.0.0-192.168.255.255 Port 53960 Zone L3-Trust Interface ethernet1/3	User Address 203.0.113.11 Country 203.0.113.0-203.0.113.255 Port 53 Zone L3-DMZ Interface ethernet1/2
	Details	Flags
	Bytes 404 Bytes Received 334 Bytes Sent 70 Repeat Count 1 Packets 2 Packets Received 1 Packets Sent 1	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP Receive Time Type Application Action Rule Bytes Category

2018/03/26 07:33:42	end	dns	allow	to-DNS-Svr-from-Trust	404	any
---------------------	-----	-----	-------	-----------------------	-----	-----

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 6197 Action allow Action Source from-policy Application web-browsing Rule Trust-to-Untrust Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/04/02 10:01:26 Start Time 2018/04/02 10:01:10 Receive Time 2018/04/02 10:01:26 Elapsed Time(sec) 0	User Address 192.168.1.101 Country 192.168.0.0-192.168.2... Port 56760 Zone L3-Trust Interface ethernet1/3 NAT IP 203.0.113.8 NAT Port 8886	User Address 183.79.248.124 Country Japan Port 80 Zone L3-Untrust Interface ethernet1/1 NAT IP 183.79.248.124 NAT Port 80

Details

Bytes 8686	Bytes Received 7786	Bytes Sent 900
Repeat Count 1	Packets 20	Packets Received 9
Packets Sent 11		

Flags

<input type="checkbox"/> Selective Portal
<input type="checkbox"/> Proxy Transaction
<input type="checkbox"/> Decryption
<input type="checkbox"/> Packet Capture
<input type="checkbox"/> Client to Server
<input type="checkbox"/> Server to Client
<input type="checkbox"/> Symmetric Return
<input type="checkbox"/> Mirrored

PCAP

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/04/02 10:01:26	end	web-browsing	allow	Trust-to-Untrust	8686	any

Close

[該当NATポリシー設定の抜粋] ※参考

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/1

IP Address: None

Destination Address Translation

Translated Address: []

Translated Port: [1 - 65535]

OK Cancel

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

設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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

Detailed Log View

General	Source	Destination
Session ID: 5317 Action: allow Action Source: from-policy Application: web-browsing Rule: Trust-to-Untrust Session End Reason: tcp-fin Category: any Virtual System: Device SN: IP Protocol: tcp Log Action: Generated Time: 2018/04/02 07:33:56 Start Time: 2018/04/02 07:33:41 Receive Time: 2018/04/02 07:33:56 Elapsed Time(sec): 0	User: 192.168.1.101 Country: 192.168.0.0-192.168.2... Port: 49834 Zone: L3-Trust Interface: ethernet1/3 NAT IP: 203.0.113.9 NAT Port: 62303	User: 183.79.250.251 Country: Japan Port: 80 Zone: L3-Untrust Interface: ethernet1/1 NAT IP: 183.79.250.251 NAT Port: 80

Details

BYTES	FLAGS
Bytes: 8686 Bytes Received: 7786 Bytes Sent: 900 Repeat Count: 1 Packets: 20 Packets Received: 9 Packets Sent: 11	<input type="checkbox"/> Active Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decryption <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored

PCAP | Receive Time | Type | Application | Action | Rule | Bytes | Category

2018/04/02 07:33:56	end	web-browsing	allow	Trust-to-Untrust	8686	any
---------------------	-----	--------------	-------	------------------	------	-----

[該当NATポリシー設定の抜粋] ※参考

NAT Policy Rule

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Translated Address

Translated Address: 203.0.113.9

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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

設定例 1

設定例 2

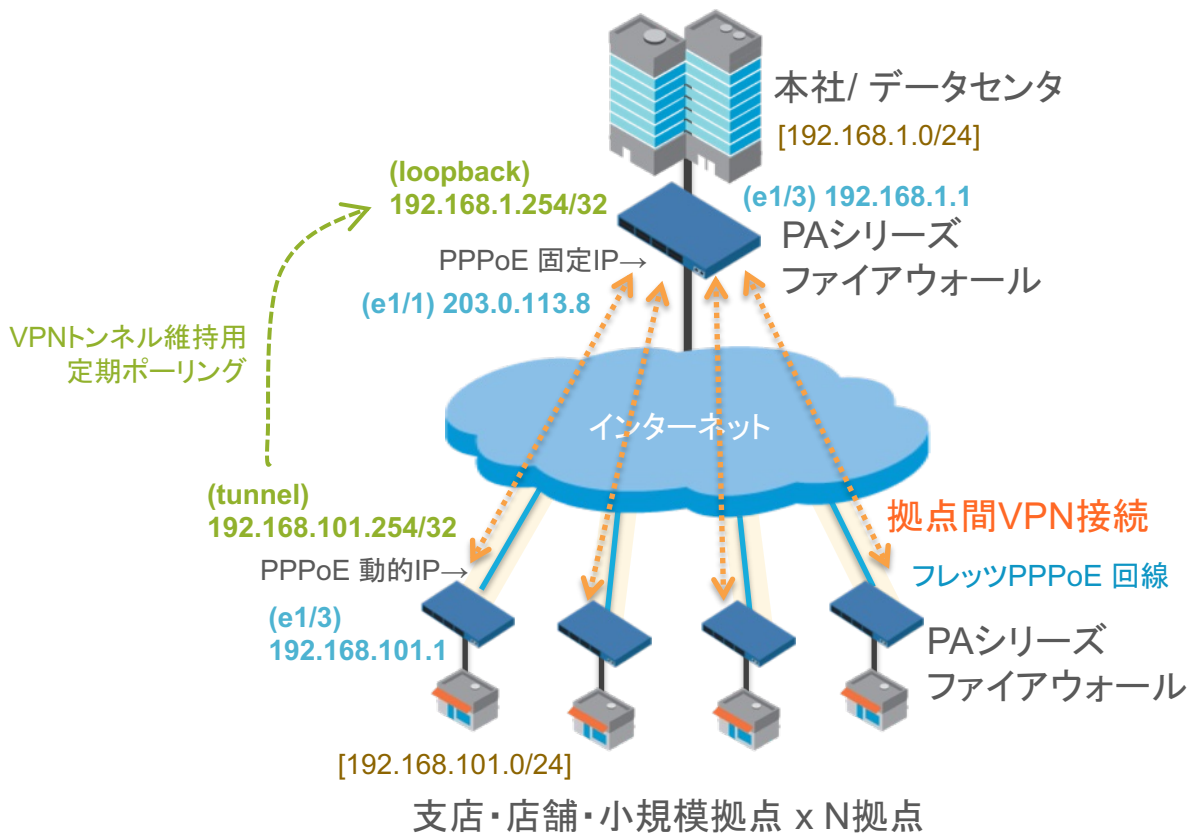
設定例 3

設定例 4

設定例 5

設定例 6

システム構成:



設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

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	<ul style="list-style-type: none">・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	<ul style="list-style-type: none">・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)

Interface Management Profile

Name

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

設定例 1

設定例 2

設定例 3

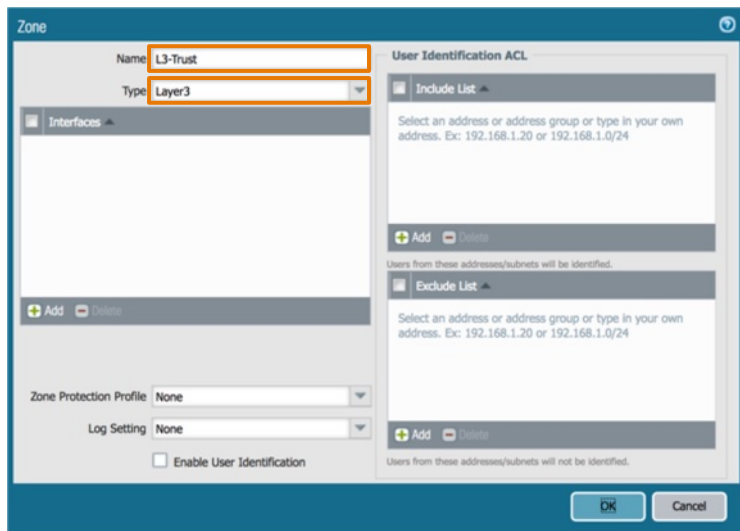
設定例 4

設定例 5

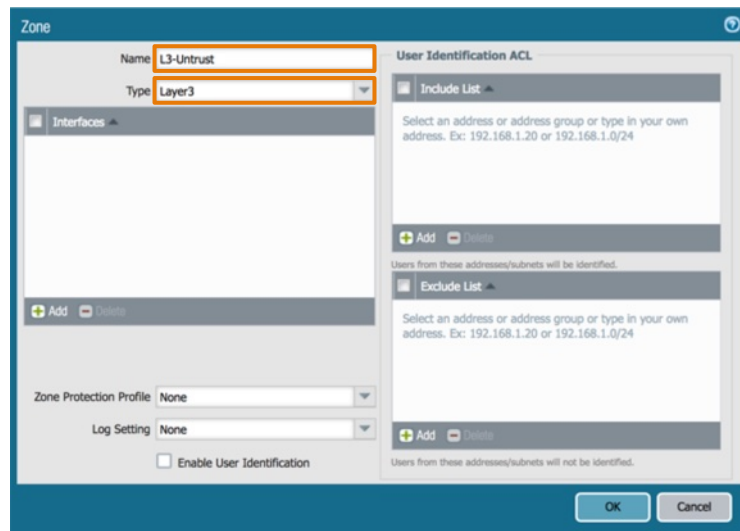
設定例 6

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)



The screenshot shows the configuration window for a security zone named "L3-Trust". The "Name" field is "L3-Trust" and the "Type" is "Layer3". The "User Identification ACL" section is empty, with "Include List" and "Exclude List" sections. The "Zone Protection Profile" is set to "None" and the "Log Setting" is also "None". The "Enable User Identification" checkbox is unchecked. The "OK" and "Cancel" buttons are at the bottom.



The screenshot shows the configuration window for a security zone named "L3-Untrust". The "Name" field is "L3-Untrust" and the "Type" is "Layer3". The "User Identification ACL" section is empty, with "Include List" and "Exclude List" sections. The "Zone Protection Profile" is set to "None" and the "Log Setting" is also "None". The "Enable User Identification" checkbox is unchecked. The "OK" and "Cancel" buttons are at the bottom.

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)

The screenshot shows the 'Zone' configuration window in Palo Alto Networks. The 'Name' field is 'L3-Tunnel' and the 'Type' is 'Layer3'. The 'Zone Protection Profile' is 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'User Identification ACL' section is empty.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The image displays three overlapping screenshots from the Palo Alto Networks configuration interface. The background screenshot shows the 'Virtual Router - default' configuration page, with the 'Static Routes' tab selected. The middle screenshot is a modal dialog titled 'Virtual Router - Static Route - IPv4' where the following fields are highlighted with orange boxes: Name (remote-101-net), Destination (192.168.101.0/24), Interface (tunnel), and Next Hop (None). The foreground screenshot shows the 'Static Routes' table with one entry: remote-101-net, Destination 192.168.101.0/24, Interface tunnel, and Next Hop default. Green arrows indicate the flow from the main configuration to the dialog and then to the updated table.

Name	Destination	Interface	Type	Val...	Next Hop	Admin Distance	Me...	BFD	No Ins...
remote-101-net	192.168.101.0/24	tunnel			default	10	None		

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name ethernet1/3

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 IPv6 Advanced

Assign Interface To

Virtual Router default

Security Zone L3-Trust

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Config' tab is selected, and the 'IPv4' sub-tab is active. Under the 'Type' section, 'Static' is selected. A table below shows one IP address entry: '192.168.1.1/24', which is highlighted with an orange box. At the bottom of the table are buttons for 'Add', 'Delete', 'Move Up', and 'Move Down'. The 'OK' and 'Cancel' buttons are at the bottom right of the window.

IP
192.168.1.1/24

IP address/netmask. Ex. 192.168.2.254/24

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/3

Comment: [Empty]

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Untrust'. The 'Config' tab is active, with sub-tabs for 'IPv4' and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
Config	IPv4 Advanced
Assign Interface To	
Virtual Router	default
Security Zone	L3-Untrust

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | **Advanced**

Type: Static **PPPoE** DHCP Client

General | **Advanced**

Enable

Username: fixed-ip-user1@pppoelab.local

Password:

Confirm Password:

Show PPPoE Client Runtime Info

OK Cancel

PPPoE を選択

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 Advanced

Type Static PPPoE DHCP Client

General Advanced

Authentication auto

Static Address None

automatically create default route pointing to peer

Default Route Metric [1 - 65535]

Access Concentrator

Service

Passive

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface

OK | Cancel

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-Tunnel

OK Cancel

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

IP

Tunnel インターフェイスには IP アドレスは設定しない
(デフォルト設定のまま)

+ Add - Delete Move Up Move Down

OK Cancel

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | **Advanced**

Other Info

Management Profile: None

MTU: [576 - 1500]

デフォルト設定のまま

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Loopback Interface

Interface Name: loopback

Comment:

Netflow Profile: None

Config: IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-Tunnel

OK Cancel

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Loopback Interface

Interface Name: loopback

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

IP
<input checked="" type="checkbox"/> 192.168.1.254/32

内部ネットワーク側と同一 IP サブネットの IP アドレスを設定

+ Add - Delete ↕ Move Up ↕ Move Down

OK Cancel

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)

The screenshot shows the 'Loopback Interface' configuration window. The 'Interface Name' is 'loopback'. The 'Netflow Profile' is 'None'. The 'Advanced' tab is selected. Under 'Other Info', the 'Management Profile' is set to 'ping-only', which is highlighted with an orange box. A callout bubble points to this dropdown with the text: '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)'. Other fields include 'MTU' (576 - 1500), 'Adjust TCP MSS' (unchecked), 'IPv4 MSS Adjustment' (40), and 'IPv6 MSS Adjustment' (60). 'OK' and 'Cancel' buttons are at the bottom.

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		

Dynamic IP Interface Status

Interface ethernet1/1
Local IP Address 203.0.113.8
Primary DNS 8.8.8.8
Secondary DNS 8.8.4.4
Primary WINS 0.0.0.0
Secondary WINS 0.0.0.0
Remote IP Address 192.0.2.254
PPPoE State Connected
PPP State Connected
Access Concentrator lab_pppoe_server
AC MAC 00:0c:29:9f:b9:b9
Authentication Method CHAP
Passive mode Disabled
Link MTU 1454

Connect Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

IKE Gateway

General | Advanced Options

Name: pa-remote-101

Version: IKEv1 only mode

Address Type: IPv4 IPv6

Interface: ethernet1/1

Local IP Address: None

Peer IP Type: Static Dynamic

Authentication: Pre-Shared Key Certificate

Pre-shared Key: [masked]

Confirm Pre-shared Key: [masked] 拠点側PAと共通のパスワードを設定

Local Identification: None

Peer Identification: User FQDN (email address) | pa@remote-site101

OK Cancel

IKE Gateway

General | Advanced Options

Common Options

Enable Passive Mode

Enable NAT Traversal

IKEv1

Exchange Mode: auto

IKE Crypto Profile: default

Enable Fragmentation

Dead Peer Detection

Interval: 5

Retry: 5

OK Cancel

Name	Peer Address	Local Address		Peer ID		Local ID		IKE Advanced Options						
		Interface	IP	ID	Type	ID	Type	Version	Mode	Passive Mode	NAT Traversal	Crypto Profile	DPD	Liveness
<input checked="" type="checkbox"/> pa-remote-101		ethernet1/1		pa@remote-site101	User FQDN (email address)			ikev1	auto	<input checked="" type="checkbox"/>	<input type="checkbox"/>	default	enabled/default/default	

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



センター側: VPN接続用 IPsec トンネル設定

- IPsec Tunnel (Network > IPsec Tunnels)

IPsec Tunnel

General Proxy IDs

Name: pa-remote-101

Tunnel Interface: tunnel

Address Type: IPv4 IPv6

Type: Auto Key Manual Key GlobalProtect Satellite

IKE Gateway: pa-remote-101

IPsec Crypto Profile: default

Show Advanced Options

Enable Replay Protection

Copy TOS Header

Tunnel Monitor

Destination IP: [Empty]

Profile: None

OK Cancel

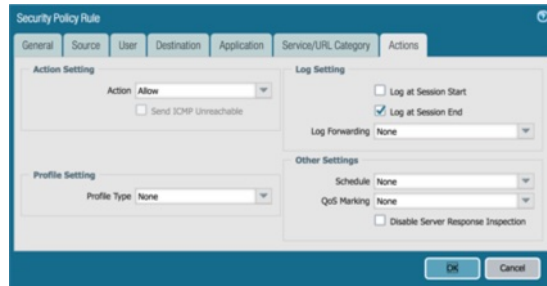
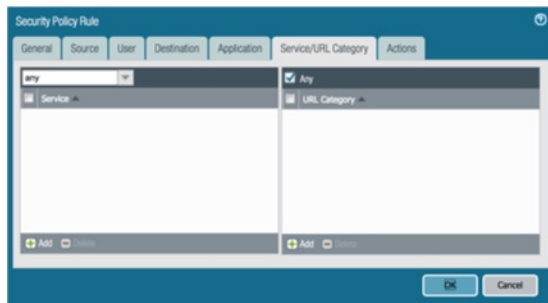
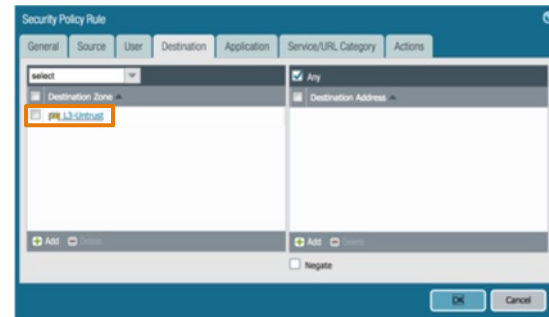
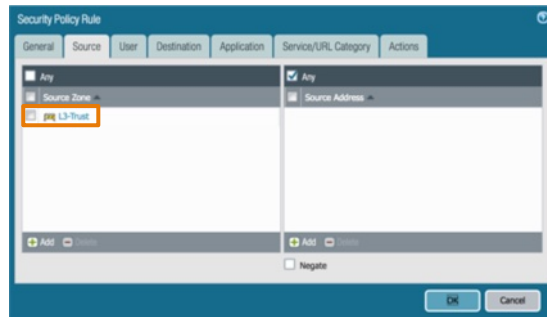
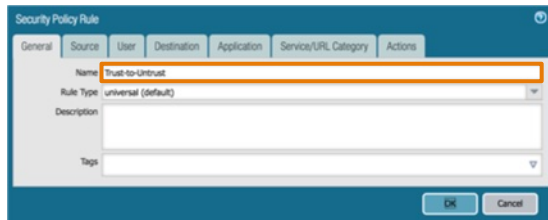
Name	Status	Type	IKE Gateway/Satellite				Tunnel Interface				
			Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
pa-remote-101	Tunnel Info	Auto Key	ethernet1/1		dynamic	IKE Info	tunnel	default (Show Routes)	vsys1	L3-Tunnel	

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



センター側：セキュリティポリシー設定

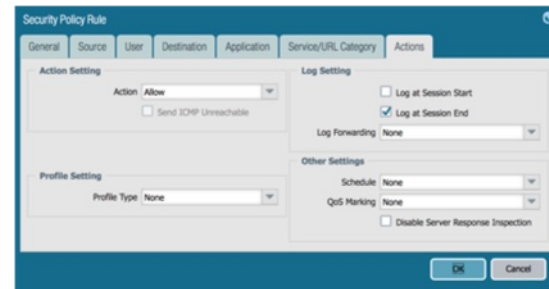
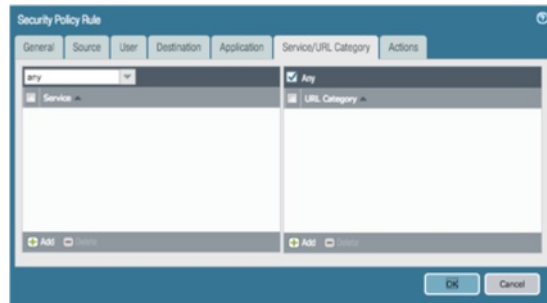
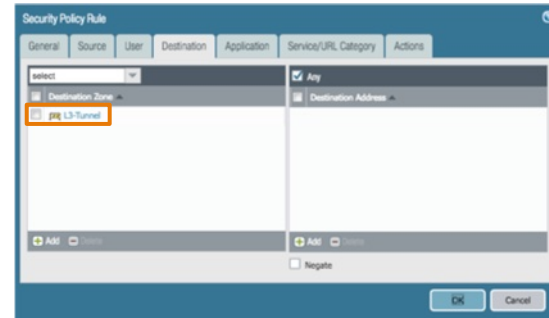
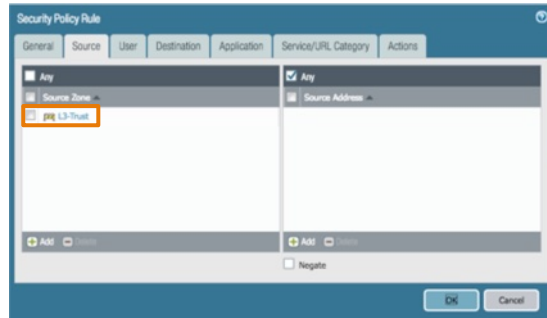
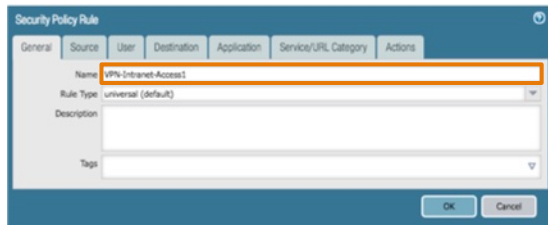
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

センター側：セキュリティポリシー設定

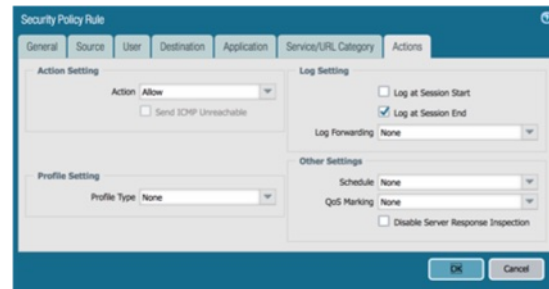
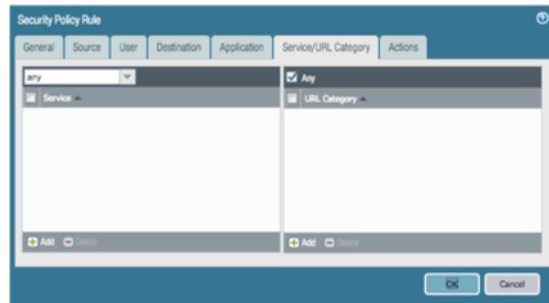
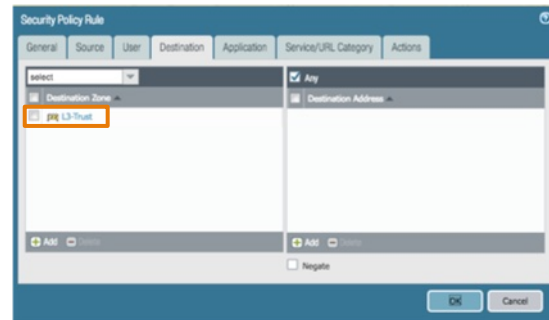
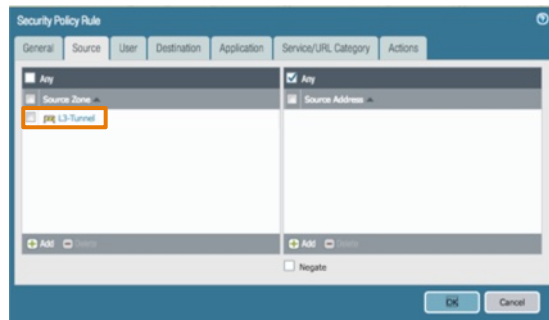
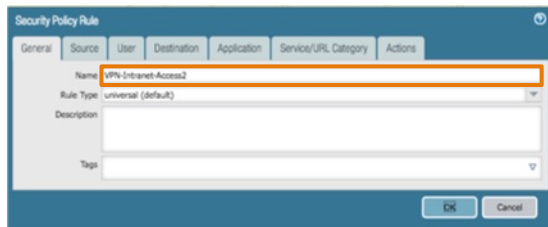
- リモート拠点向けVPN通信用セキュリティポリシーの設定1 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)

	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	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		intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default		interzone	any	any	any	any	any	any	any	Deny	none	none

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

NAT Policy Rule configuration window, General tab. The Name field is set to "N to 1 NAT" and is highlighted with an orange box. The NAT Type is set to "IPv4".

NAT Policy Rule configuration window, Original Packet tab. The Destination Zone is set to "L3-Untrust" and is highlighted with an orange box. The Source Zone is set to "L3-Trust" and is also highlighted with an orange box. The Destination Interface is set to "any".

NAT Policy Rule configuration window, Translated Packet tab. The Source Address Translation section is highlighted with an orange box. The Translation Type is set to "Dynamic IP And Port", Address Type is "Interface Address", Interface is "ethernet1/1", and IP Address is "None". The Destination Address Translation section is also visible, with Translated Address set to "any" and Translated Port set to "[1 - 65535]".

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)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

設定例 1

設定例 2

設定例 3

設定例 4

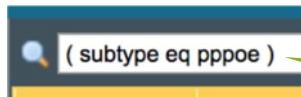
設定例 5

設定例 6

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@pppoeab.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@pppoeab.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

設定例 1

設定例 2

設定例 3

設定例 4

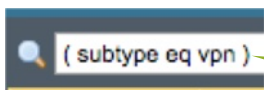
設定例 5

設定例 6

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.



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

Detailed Log View

General	Source	Destination
Session ID 10453 Action allow Action Source from-policy Application ssh Rule VPN-Intranet-Access1 Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/26 15:27:49 Start Time 2018/03/26 15:27:23 Receive Time 2018/03/26 15:27:49 Elapsed Time(sec) 11	User Address 192.168.1.102 Country 192.168.0.0-192.168.2... Port 51306 Zone L3-Trust Interface ethernet1/3	User Address 192.168.101.101 Country 192.168.0.0-192.168.2... Port 22 Zone L3-Tunnel Interface tunnel

Details	Flags
Bytes 18642 Bytes Received 9403 Bytes Sent 9239 Repeat Count 1 Packets 140 Packets Received 55 Packets Sent 85	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	URL	File Name
	2018/03/26 15:27:49	end	ssh	allow	VPN-Intranet-Access1	18642		any		

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 10445 Action allow Action Source from-policy Application ssh Rule VPN-Intranet-Access2 Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/26 15:24:03 Start Time 2018/03/26 15:23:44 Receive Time 2018/03/26 15:24:03 Elapsed Time(sec) 4	User 192.168.101.101 Address 192.168.101.101 Country 192.168.0.0-192.168.2... Port 40068 Zone L3-Tunnel Interface tunnel	User 192.168.1.102 Address 192.168.1.102 Country 192.168.0.0-192.168.2... Port 22 Zone L3-Trust Interface ethernet1/3

Details	Flags
Bytes 9072 Bytes Received 4671 Bytes Sent 4401 Repeat Count 1 Packets 53 Packets Received 25 Packets Sent 28	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	URL	File Name
	2018/03/26 15:24:03	end	ssh	allow	VPN-Intranet-Access2	9072		any		

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Interface Management Profile

Name

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

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)

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Trust'. The 'Name' field is 'L3-Trust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty, with 'Include List' and 'Exclude List' sections. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

The screenshot shows the 'Zone' configuration window for a zone named 'L3-Untrust'. The 'Name' field is 'L3-Untrust' and the 'Type' is 'Layer3'. The 'User Identification ACL' section is empty, with 'Include List' and 'Exclude List' sections. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom.

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The screenshot shows the 'Zone' configuration window in Palo Alto Networks. The 'Name' field is 'L3-Tunnel' and the 'Type' is 'Layer3'. The 'Zone Protection Profile' is set to 'None' and the 'Log Setting' is 'None'. The 'Enable User Identification' checkbox is unchecked. The 'User Identification ACL' section is visible on the right side of the window.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The image displays three overlapping screenshots from the Palo Alto Networks configuration interface, illustrating the steps to add a static route to a virtual router.

Left Screenshot: Shows the 'Virtual Router - default' configuration page. The 'Name' field is set to 'default'. The 'Static Routes' tab is selected in the left-hand menu. The 'Administrative Distances' section is visible, with 'Static' set to 10.

Middle Screenshot: A modal dialog titled 'Virtual Router - Static Route - IPv4' is open. The fields are filled with: Name: hq-net, Destination: 192.168.1.0/24, Interface: tunnel, Next Hop: None (selected), Admin Distance: (empty), Metric: 10, and BFD Profile: None. Green arrows point from this dialog to the other two screenshots.

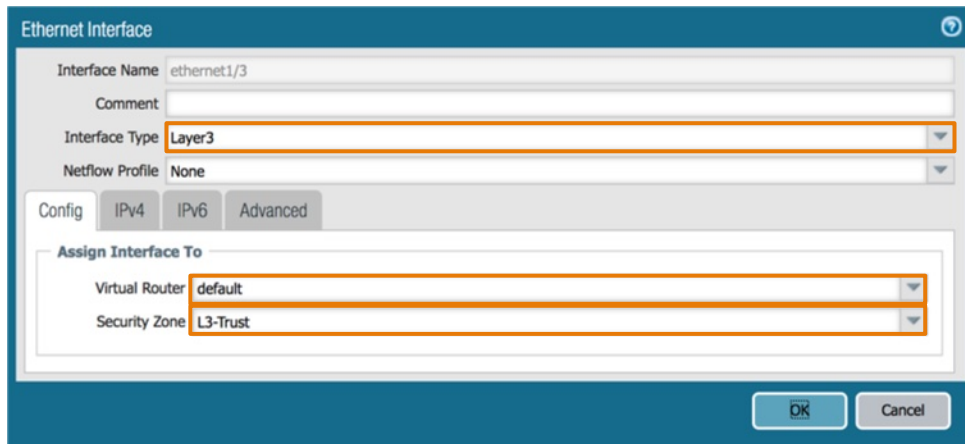
Right Screenshot: Shows the 'Virtual Router - default' configuration page with the 'Static Routes' tab selected. A table displays the added route:

Name	Destination	Interface	Next Hop		Admin Distance	Metric	BFD	No Install
			Type	Value				
hq-net	192.168.1.0/24	tunnel			default	10	None	

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Trust'. The 'Config' tab is selected, and the 'OK' and 'Cancel' buttons are visible at the bottom.

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-Trust

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Type' is set to 'Static'. Under the 'IP' section, the address '192.168.101.1/24' is listed and highlighted with an orange box. The 'Add', 'Delete', 'Move Up', and 'Move Down' buttons are visible at the bottom of the IP list. The 'OK' and 'Cancel' buttons are at the bottom right of the window.

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Type: Static PPPoE DHCP Client

IP

192.168.101.1/24

Add Delete Move Up Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/3

Comment: []

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Untrust'. The 'Config' tab is active, with sub-tabs for 'IPv4' and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom.

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
Assign Interface To	
Virtual Router	default
Security Zone	L3-Untrust

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Type: Static PPPoE DHCP Client

General | Advanced

Enable

Username: dyn-ip-user101@pppoelab.local

Password: *****

Confirm Password: *****

Show PPPoE Client Runtime Info

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 Advanced

Type Static PPPoE DHCP Client

General Advanced

Authentication auto

Static Address None

automatically create default route pointing to peer

Default Route Metric [1 - 65535]

Access Concentrator

Service

Passive

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface

OK | Cancel

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)

The screenshot shows the 'Tunnel Interface' configuration window. The 'Interface Name' is set to 'tunnel'. The 'Netflow Profile' is set to 'None'. The 'Assign Interface To' section has two dropdown menus: 'Virtual Router' is set to 'default' and 'Security Zone' is set to 'L3-Tunnel'. The 'Config' tab is active, and the 'Advanced' sub-tab is selected. The 'OK' and 'Cancel' buttons are visible at the bottom.

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config: IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-Tunnel

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

IP
<input type="checkbox"/> 192.168.101.254/32

VPN 接続維持用 ポーリング用にIPアドレスを設定
※LAN側サブネットと同一のネットワークアドレス(/32マスク)

+ Add - Delete ↕ Move Up ↕ Move Down

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Other Info

Management Profile: ping-only

MTU: [576 - 1500]

OK Cancel

ICMP 疎通確認のための設定 (オプション)

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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		

Dynamic IP Interface Status

Interface: ethernet1/1

Local IP Address: 198.51.100.102

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.4.4

Primary WINS: 0.0.0.0

Secondary WINS: 0.0.0.0

Remote IP Address: 192.0.2.254

PPPoE State: Connected

PPP State: Connected

Access Concentrator: lab_pppoe_server

AC MAC: 00:0c:29:9f:b9:b9

Authentication Method: CHAP

Passive mode: Disabled

Link MTU: 1454

Connect Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



拠点側: VPN接続用 IPsec IKE ゲートウェイ設定

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

IKE Gateway

General Advanced Options

Name

Version

Address Type IPv4 IPv6

Interface

Local IP Address

Peer IP Type Static Dynamic

Peer IP Address

Authentication Pre-Shared Key Certificate

Pre-shared Key

Confirm Pre-shared Key

Local Identification

Peer Identification

OK Cancel

センター側PAと共通のパスワードを設定

IKE Gateway

General Advanced Options

Common Options

Enable Passive Mode

Enable NAT Traversal

IKEv1

Exchange Mode

IKE Crypto Profile

Enable Fragmentation

Dead Peer Detection

Interval

Retry

OK Cancel

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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PAに設定したLoopbackアドレス

Network > Network Profiles > Monitor

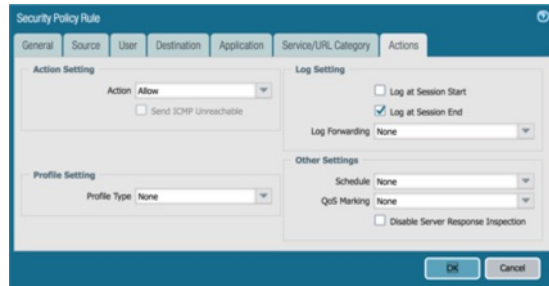
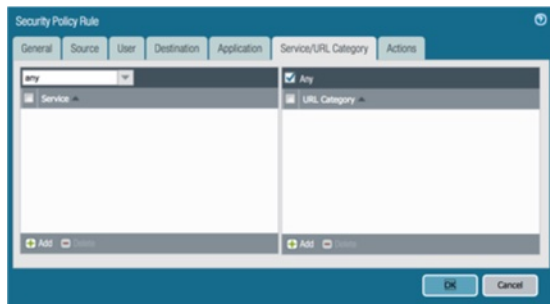
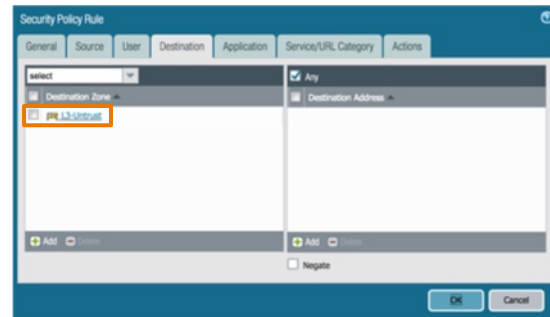
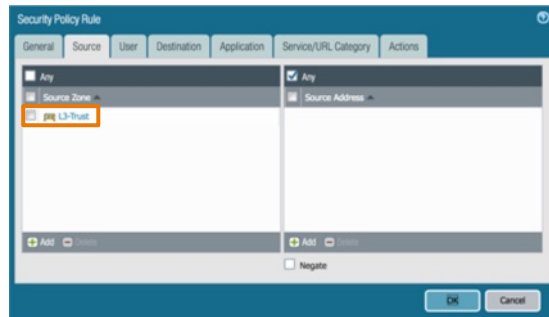
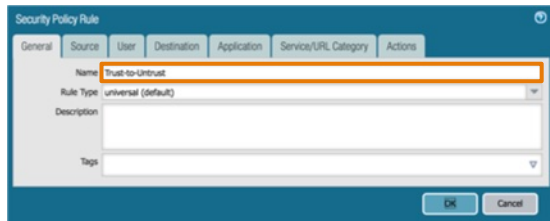
Name	Status	Type	IKE Gateway/Satellite				Tunnel Interface				
			Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
pa-hq-01	Tunnel Info	Auto Key	ethernet1/1		203.0.113.8	IKE Info	tunnel	default (Show Routes)	vsys1	L3-Tunnel	OK

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



拠点側: セキュリティポリシー設定

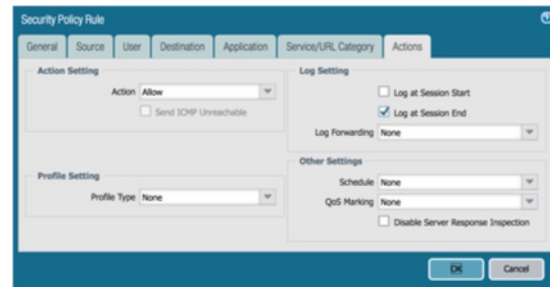
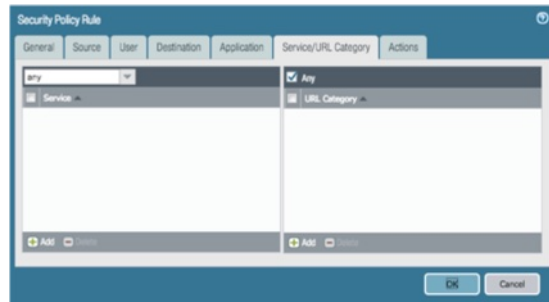
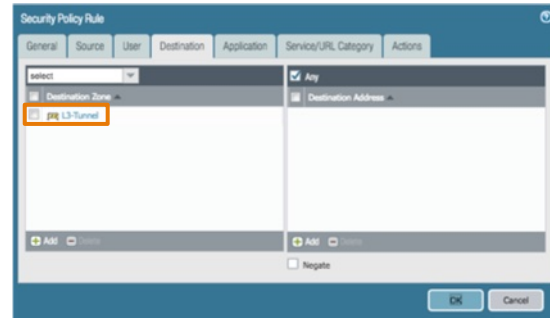
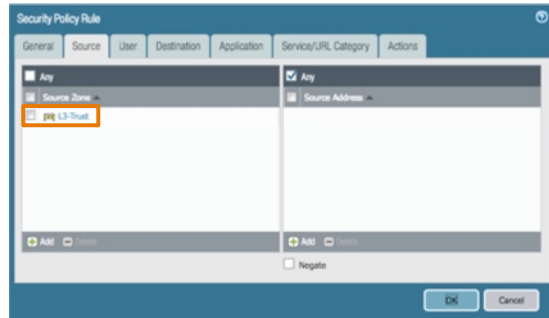
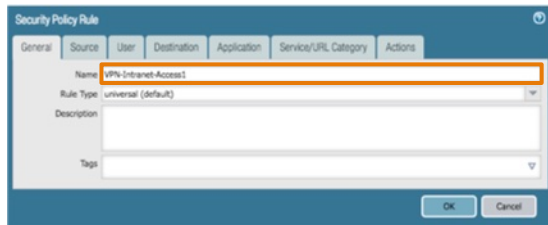
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

拠点側: セキュリティポリシー設定

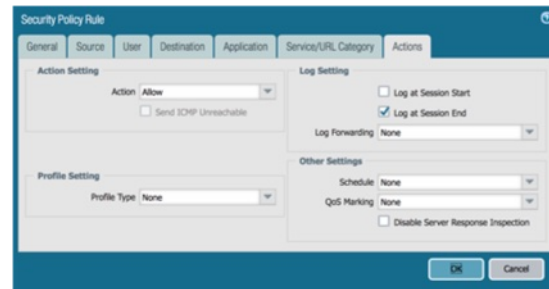
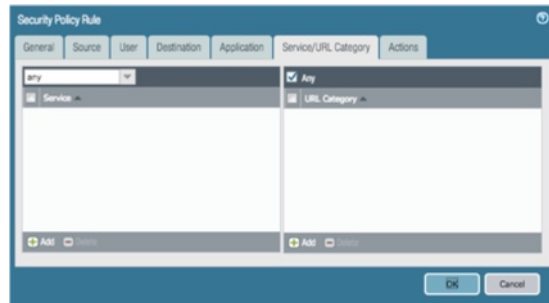
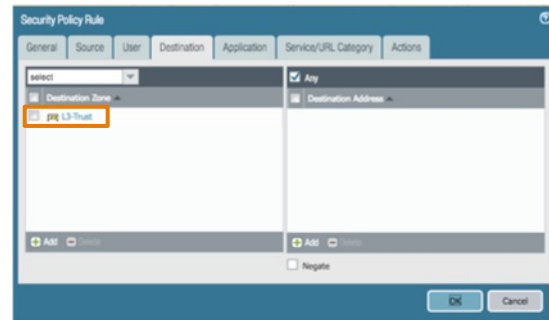
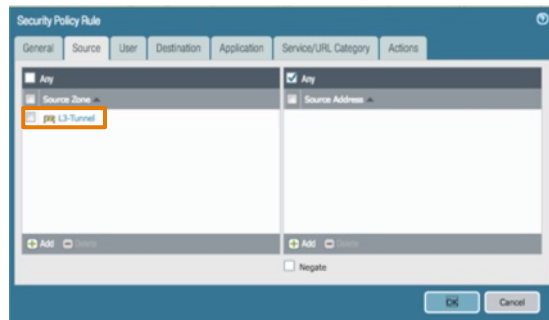
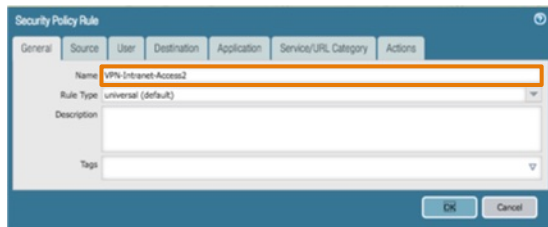
- センター拠点向けVPN通信用セキュリティポリシーの設定1 (Policies > Security)



設定例1
設定例2
設定例3
設定例4
設定例5
設定例6

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)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

	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	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		intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	none
5	interzone-default		interzone	any	any	any	any	any	any	any	Deny	none	none

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

NAT Policy Rule configuration window, General tab. The Name field is set to "N to 1 NAT" and is highlighted with an orange box. The NAT Type is set to "IPv4".

NAT Policy Rule configuration window, Original Packet tab. The Destination Zone is set to "L3-Untrust" and is highlighted with an orange box. The Source Zone is set to "L3-Trust" and is also highlighted with an orange box. The Destination Interface is set to "any" and the Service is set to "any".

NAT Policy Rule configuration window, Translated Packet tab. The Source Address Translation section is active. The Translation Type is set to "Dynamic IP And Port", Address Type is "Interface Address", Interface is "ethernet1/1", and IP Address is "None". These four fields are highlighted with orange boxes. The Destination Address Translation section is disabled. A green callout bubble points to the IP Address field.

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

拠点側: **NAT**ポリシー設定一覧

- NATポリシー設定一覧 (Policies > NAT)

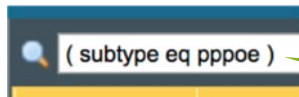
	Name	Original Packet						Translated Packet	
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	N to 1 NAT	L3-Trust	L3-Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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



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

設定例 1

設定例 2

設定例 3

設定例 4

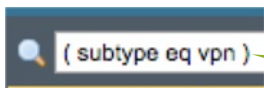
設定例 5

設定例 6

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 14334 Action allow Action Source from-policy Application ssh Rule VPN-Intranet-Access1 Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/26 15:24:02 Start Time 2018/03/26 15:23:45 Receive Time 2018/03/26 15:24:02 Elapsed Time(sec) 3	User Address 192.168.101.101 Country 192.168.0.0-192.168.2... Port 40068 Zone L3-Trust Interface ethernet1/3	User Address 192.168.1.102 Country 192.168.0.0-192.168.2... Port 22 Zone L3-Tunnel Interface tunnel
	Details	Flags
	Bytes 9048 Bytes Received 4871 Bytes Sent 4177 Repeat Count 1 Packets 53 Packets Received 25 Packets Sent 28	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/26 15:24:02	end	ssh	allow	VPN-intranet-Access1	9048	any

Close

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

Detailed Log View

General	Source	Destination
Session ID 14341 Action allow Action Source from-policy Application ssh Rule VPN-Intranet-Access2 Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/26 15:27:49 Start Time 2018/03/26 15:27:23 Receive Time 2018/03/26 15:27:49 Elapsed Time(sec) 12	User Address 192.168.1.102 Country 192.168.0.0-192.168.2... Port 51306 Zone L3-Tunnel Interface tunnel	User Address 192.168.101.101 Country 192.168.0.0-192.168.2... Port 22 Zone L3-Trust Interface ethernet1/3
	Details	Flags
	Bytes 18882 Bytes Received 8963 Bytes Sent 9919 Repeat Count 1 Packets 140 Packets Received 55 Packets Sent 85	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/26 15:27:49	end	ssh	allow	VPN-Intranet-Access2	18882	any

Close

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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

設定例 1

設定例 2

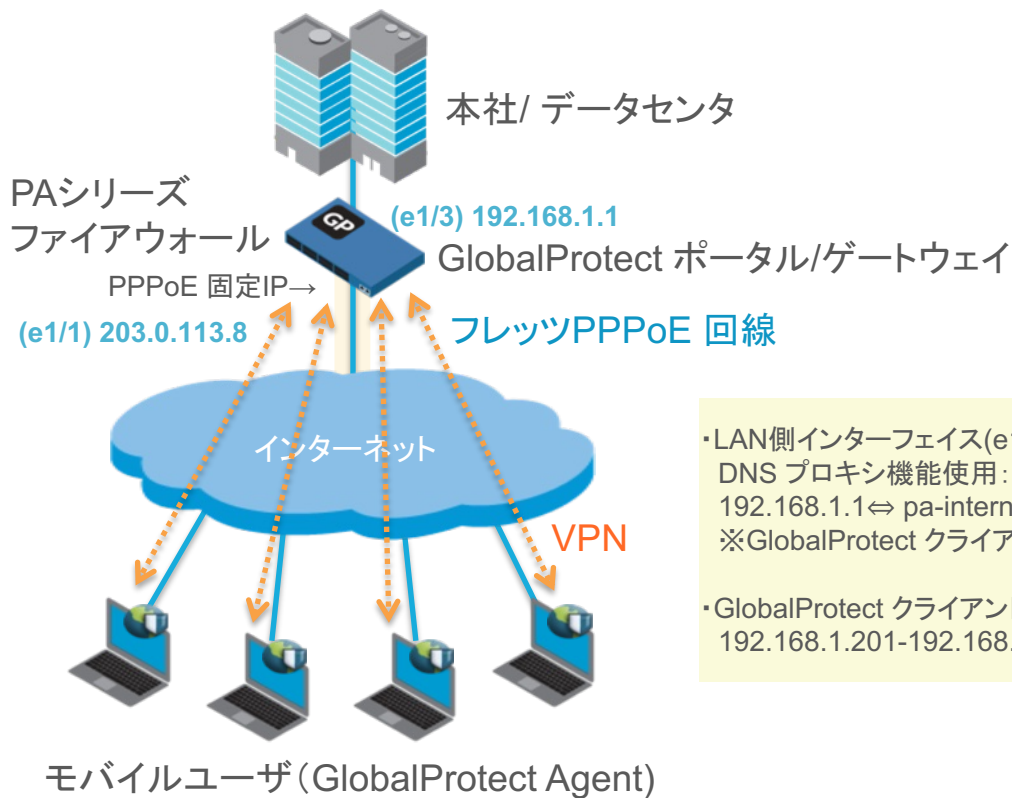
設定例 3

設定例 4

設定例 5

設定例 6

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	<ul style="list-style-type: none">・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	<ul style="list-style-type: none">・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)

GlobalProtect Portal/External Gateway用インターネット側 I/Fアドレス

GlobalProtect Internal Gateway PA LAN 側 I/Fアドレス

Name	Subject	Issuer	CA	Key	Expires	Status	Algorit...	Usage
CA-for-PPPoE-Lab	CN = CA-for-PPPoE-Lab	CN = CA-for-PPPoE-Lab	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 26 08:09:12 2019 GMT	valid	RSA	
Cert-for-GP-Int-GW	CN = 192.168.1.1	CN = CA-for-PPPoE-Lab	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 26 23:38:09 2019 GMT	valid	RSA	

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Certificate Profile

Name:

Username Field:

User Domain:

<input type="checkbox"/>	Name	Default OCSP URL	OCSP Verify CA
<input checked="" type="checkbox"/>	CA-for-PPPoE-Lab		

Default OCSP URL (must start with http:// or https://)

Use CRL
OCSP takes precedence over CRL

CRL Receive Timeout (sec)

Use OCSP

OCSP Receive Timeout (sec)

Certificate Status Timeout (sec)

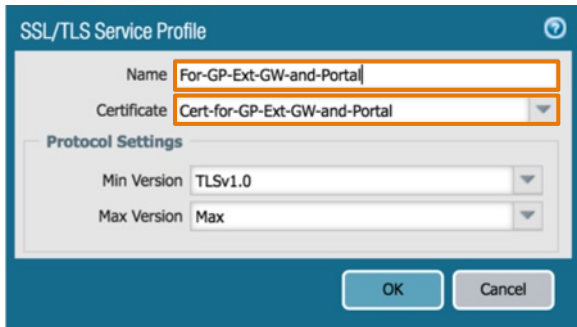
Block session if certificate status is unknown

Block session if certificate status cannot be retrieved within timeout

Block session if the certificate was not issued to the authenticating device

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)



SSL/TLS Service Profile

Name: For-GP-Ext-GW-and-Portal

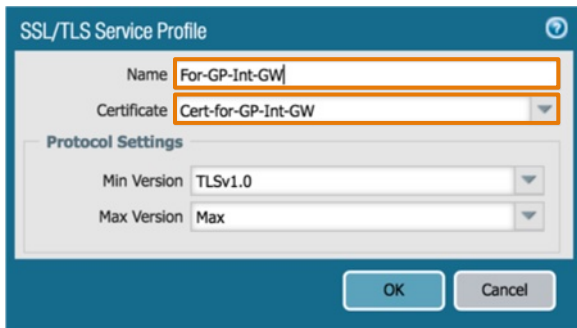
Certificate: Cert-for-GP-Ext-GW-and-Portal

Protocol Settings

Min Version: TLSv1.0

Max Version: Max

OK Cancel



SSL/TLS Service Profile

Name: For-GP-Int-GW

Certificate: Cert-for-GP-Int-GW

Protocol Settings

Min Version: TLSv1.0

Max Version: Max

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Local User

Name: GPUser01

Mode: Password Password Hash

Password: *****

Confirm Password: *****

Enable

OK Cancel

Local User

Name: GPUser02

Mode: Password Password Hash

Password: *****

Confirm Password: *****

Enable

OK Cancel

Local User

Name: GPUser03

Mode: Password Password Hash

Password: *****

Confirm Password: *****

Enable

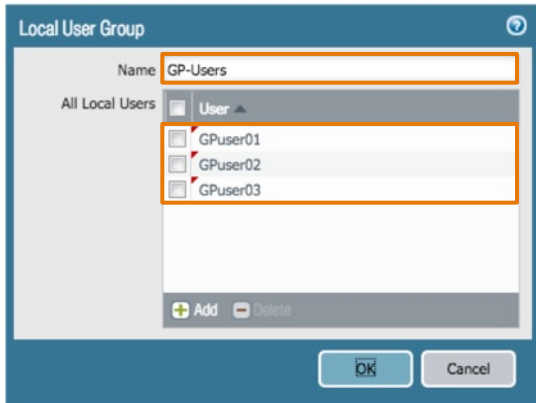
OK Cancel

<input type="checkbox"/>	Name	Location	Enabled
<input type="checkbox"/>	GPUser01		<input checked="" type="checkbox"/>
<input type="checkbox"/>	GPUser02		<input checked="" type="checkbox"/>
<input type="checkbox"/>	GPUser03		<input checked="" type="checkbox"/>

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)



<input type="checkbox"/>	Name	Location	Local Users
<input type="checkbox"/>	GP-Users		GPUser01 GPUser02 GPUser03

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Authentication Profile

Name: Auth-Profile-for-GP

Authentication: Basic

Type: Local Database

User Domain:

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field X Import

OK Cancel

Authentication Profile

Name: Auth-Profile-for-GP

Authentication: Advanced

Allow List

- GP-Users

Account Lockout

Failed Attempts: 0

Lockout Time (min): 0

OK Cancel

	Name	Location	Lockout		Allow List	Authentication	Server Profile	Others	Locked Users
			Failed Attempts (#)	Lockout Time (min)					
<input checked="" type="checkbox"/>	Auth-Profile-for-GP		0 (default)	0 (default)	GP-Users	Local			none

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Interface Management Profile

Name: ping-only

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

設定例 1

設定例 2

設定例 3

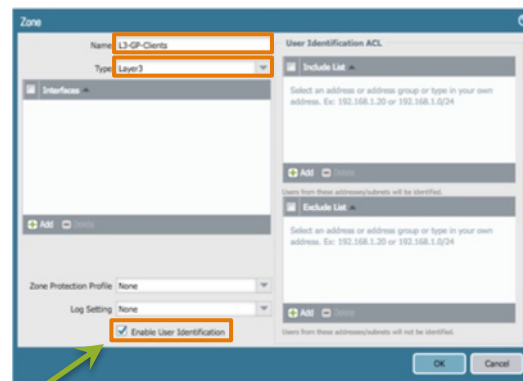
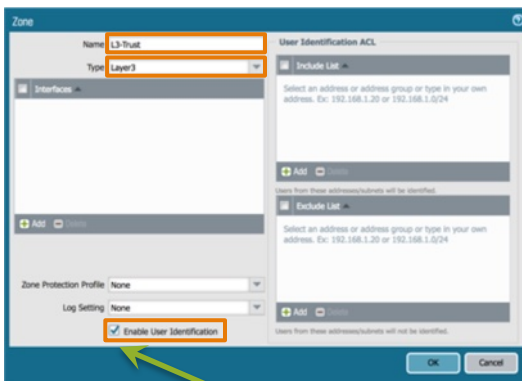
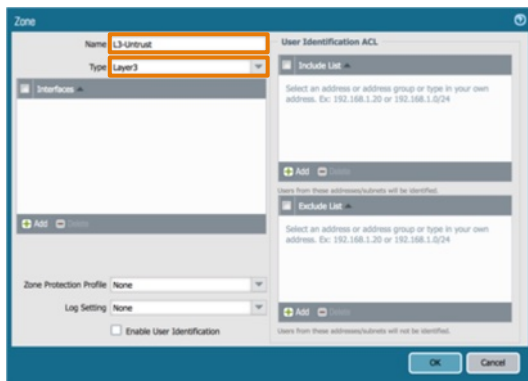
設定例 4

設定例 5

設定例 6

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. Below these fields are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced'. The 'Assign Interface To' section contains two dropdown menus: 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Trust'. 'OK' and 'Cancel' buttons are at the bottom right.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Config' tab is selected, and the 'IPv4' sub-tab is active. Under the 'Type' section, 'Static' is selected. A table lists the IP address '192.168.1.1/24', which is highlighted with an orange box. Below the table are buttons for 'Add', 'Delete', 'Move Up', and 'Move Down'. The footer text reads 'IP address/netmask. Ex. 192.168.2.254/24'. 'OK' and 'Cancel' buttons are at the bottom right.

IP
192.168.1.1/24

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)

The screenshot shows the configuration page for an Ethernet Interface named 'ethernet1/3'. The interface type is 'Layer3' and the netflow profile is 'None'. The 'Advanced' tab is selected, showing 'Link Settings' (Link Speed: auto, Link Duplex: auto, Link State: auto) and 'Other Info' (ARP Entries, ND Entries, NDP Proxy, LLDP). The 'Management Profile' dropdown menu is highlighted with an orange box and set to 'ping-only'. Below it, the MTU is set to [576 - 1500]. There are also fields for 'Adjust TCP MSS' (IPv4 MSS Adjustment: 40, IPv6 MSS Adjustment: 60) and an 'Untagged Subinterface' checkbox.

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Untrust'. The 'Config' tab is active, with sub-tabs for 'IPv4' and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
Config	IPv4 Advanced
Assign Interface To	
Virtual Router	default
Security Zone	L3-Untrust

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | **Advanced**

Type: Static **PPPoE** DHCP Client

General | **Advanced**

Enable

Username: fixed-ip-user1@pppoelab.local

Password:

Confirm Password:

Show PPPoE Client Runtime Info

OK Cancel

PPPoE を選択

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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Type: Static PPPoE DHCP Client

General | Advanced

Authentication: auto

Static Address: 203.0.113.8

automatically create default route pointing to peer

Default Route Metric: [1 - 65535]

Access Concentrator:

Service:

Passive

OK Cancel

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface

OK Cancel

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)

The screenshot shows the 'Tunnel Interface' configuration window. The 'Interface Name' is set to 'tunnel'. The 'Netflow Profile' is set to 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-GP-Clients'. The 'Config' tab is active, with sub-tabs for 'IPv4', 'IPv6', and 'Advanced'. The 'OK' and 'Cancel' buttons are visible at the bottom.

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config: IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: L3-GP-Clients

OK Cancel

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

IP

Tunnel インターフェイスには IP アドレスは設定しない
(デフォルト設定のまま)

+ Add - Delete ↻ Move Up ↻ Move Down

OK Cancel

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)

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | **Advanced**

Other Info

Management Profile: None

MTU: [576 - 1500] デフォルト設定のまま

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Interface: ethernet1/3
Mode: enabled

Lease Options

Ping IP when allocating new IP

Lease: Unlimited Timeout

1 Days 0 Hours 0 Minutes

IP Pools	Reserved Address	MAC Address
192.168.1.101-192.168.1.110	192.168.1.20	XXXXXXXXXXXX (Optional MAC Address)

Buttons: Add, Delete, OK, Cancel

内部側ネットワークのクライアントPC
に割り当てるIPアドレス範囲を設定

Interface: ethernet1/3
Mode: enabled

Lease Options

Inheritance Source: None

Check inheritance source status

Gateway: 192.168.1.1

Subnet Mask: 255.255.255.0

Primary DNS: 192.168.1.1

Secondary DNS: None

Primary WINS: None

Secondary WINS: None

Primary NIS: None

Secondary NIS: None

Primary NTP: None

Secondary NTP: None

POP3 Server: None

SMTP Server: None

DNS Suffix: pppoelab.local

Custom DHCP options			
Name	Code	Type	Value

Buttons: Add, Delete, Move Up, Move Down, OK, Cancel

DNS 逆引き機能を利用した GlobalProtect
クライアントの接続先ネットワーク自動判別
のための設定

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

GlobalProtect DNS Reverse Lookup用 DNS Proxy 設定

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

DNS Proxy

Enable

Name: dns-proxy-for-internal-net

Inheritance Source: None

Primary: 8.8.8.8

Secondary: 8.8.4.4

Interface: ethernet1/3

DNS Proxy Rules: Static Entries | Advanced

Name	FQDN	Address
pa-internal-ip	pa-internal-ip.pppoelab.local	192.168.1.1

OK Cancel

DNSプロキシを有効にするインターフェイス (内部ネットワーク側インターフェイス)

PA 内部LAN側クライアントからのDNSクエリ処理用のDNS A/PTRレコード

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

GlobalProtect ポータル 設定

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

GlobalProtect Portal Configuration

General

Name: GP-Portal

Authentication

Agent

Satellite

Network Settings

Interface: ethernet1/1

IP Address: 203.0.113.8

Appearance

Disable login page

Custom Login Page: None

Custom Help Page: None

OK Cancel

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ようになる

GlobalProtect ポータル 設定

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

GlobalProtect Portal Configuration

General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service Profile: For-GP-Ext-GW-and-Portal

Client Authentication

<input type="checkbox"/>	Name	OS	Authentication Profile	Authentication Message
<input checked="" type="checkbox"/>	GP-Portal-ClientAuth	Any	Auth-Profile-for-GP	Enter login credentials

+ Add - Delete Clone Move Up Move Down

Certificate Profile: None

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

GlobalProtect ポータル 設定

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

The screenshot displays the 'GlobalProtect Portal Configuration' window. On the left, a sidebar contains tabs for 'General', 'Authentication', 'Agent', and 'Satellite'. The 'Agent' tab is selected. The main area is titled 'Agent' and contains a table with the following data:

<input type="checkbox"/>	Configs	User/User Group	OS	External Gateways	Client Certificate
<input checked="" type="checkbox"/>	Agent-Config01	any	any	GP-External-GW (Highest)	

Below the table are controls: '+ Add', '- Delete', 'Clone', 'Move Up', and 'Move Down'. Underneath is a 'Trusted Root CA' section with a table:

<input type="checkbox"/>	Trusted Root CA	Install In Local Root Certificate Store
<input checked="" type="checkbox"/>	CA-for-PPPoE-Lab	<input type="checkbox"/>

Additional controls include '+ Add' and '- Delete'. To the right of this section are two text boxes: 'Agent User Override Key' and 'Confirm Agent User Override Key', both containing masked characters (****). At the bottom right are 'OK' and 'Cancel' buttons.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

GlobalProtect ポータル 設定

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

GlobalProtect Portal Configuration

General
Authentication
Agent
Satellite

Agent

- Configs
- Agent-Config01

+ Add - Delete

Trusted Root CA

CA-for-PPPoE-Lab

+ Add - Delete

Configs

Authentication User/User Group Gateways App Data Collection

Name Agent-Config01

Client Certificate None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials Yes

Authentication Override

- Generate cookie for authentication override
- Accept cookie for authentication override

Cookie Lifetime Hours 24

Certificate to Encrypt/Decrypt Cookie None

Components that Require Dynamic Passwords (Two-Factor Authentication)

- Portal
- Internal gateways-all
- External gateways-manual only
- External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

GlobalProtect ポータル 設定

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

GlobalProtect Portal Configuration

Agent

Configs

Agent-Config01

Trusted Root CA

CA-for-PPPoE-Lab

Configs

Authentication User/User Group Gateways App Data Collection

Any any

OS User/User Group

デフォルトのまま(すべてのOS, すべてのユーザからのアクセスを許可)

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

GlobalProtect ポータル 設定

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

GlobalProtect Portal Configuration

General
Authentication
Agent
Satellite

Agent
Configs
Agent-Config01

Configs

Authentication User/User Group Gateways App Data Collection

Internal Gateways

Name	Address
GP-Internal-GW	192.168.1.1

GlobalProtect 内部ゲートウェイ名とIPアドレスを設定

External Gateways

Cutoff Time (sec) 5

Name	Address	Priority	Manual
GP-External-GW	203.0.113.8	Highest	<input type="checkbox"/>

GlobalProtect 外部ゲートウェイ名とIPアドレスを設定

Internal Host Detection

IP Address 192.168.1.1

Hostname pa-internal-ip.pppoelab.local

GlobalProtect クライアントの接続先ネットワーク(内部ネットワーク or 外部)を自動判別させるための設定。本例ではクライアントのネットワーク接続後、“192.168.1.1” に対するDNS逆引きを実行し、ホスト名(FQDN) “pa-internal-ip.pppoelab.local” が返ってきた場合、内部ネットワークに接続されていると判断します。

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



GlobalProtect ポータル 設定

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

GlobalProtect Portal Configuration

General
Authentication
Agent
Satellite

Agent
Configs
Agent-Config01

Configs
Authentication User/User Group Gateways App Data Collection

App Configurations

Connect Method	User-logout (Always On)
GlobalProtect App Config Refresh Interval (hours)	24 [1 - 168]
Allow User to Disable GlobalProtect App	Allow
Allow User to Upgrade GlobalProtect App	Allow Transparently
Use Single Sign-on (Windows Only)	No
Clear Single Sign-On Credentials on Logout (Windows Only)	Yes
Use Default Authentication on Kerberos Authentication Failure (Windows Only)	Yes
Automatic Restoration of VPN Connection Timeout (min)	30 [0 - 180]
Wait Time Between VPN Connection Restore Attempts (sec)	5 [1 - 60]

Passcode

Disable Timeout (min) 0

Enrollment Port 443

OK Cancel

本構成例では未設定。ホスト状態(HIP)を元にしたアクセス制御(便利!)を行う場合に設定

本構成例では設定しない

GlobalProtect クライアントアプリケーションのアップグレード方法(透過的なアップグレード)

GlobalProtect ログインにシングルサインオンを使用するか(この例ではSSO未使用のためNoに設定)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Gateway Configuration

General Name: GP-External-GW

Authentication

Agent

Satellite

Network Settings

Interface: ethernet1/1

IP Address: 203.0.113.8

OK Cancel

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ようになる

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 Gateway Configuration

General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service Profile: For-GP-Ext-GW-and-Portal

Client Authentication

<input type="checkbox"/>	Name	OS	Authentication Profile	Authentication Message
<input checked="" type="checkbox"/>	GP-Client-Auth	Any	Auth-Profile-for-GP	Enter login credentials

+ Add - Delete Clone Move Up Move Down

Certificate Profile: None

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings **Timeout Settings** Client Settings Network Services HIP Notification

Tunnel Mode 本構成例では設定しない

Tunnel Interface: tunnel

Max User: [1 - 25]

Enable IPSec

GlobalProtect IPSec Crypto: default

Enable X-Auth Support

Group Name: _____

Group Password: _____

Confirm Group Password: _____

Skip Auth on IKE Rekey

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings | Timeout Settings | Client Settings | Network Services | HIP Notification

1 item

Configs	User/User Group	OS	IP Pool	Authentication Server IP Pool	Access Route
<input type="checkbox"/> GP-GW-Client-Config	any	any	192.168.1.201-192.168.1.210		

+ Add | - Delete | Clone | Move Up | Move Down

OK Cancel

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The screenshot displays the 'GlobalProtect Gateway Configuration' window. On the left, a sidebar contains tabs for 'General', 'Authentication', 'Agent', and 'Satellite'. The 'Configs' tab is active, showing a list of configurations with 'GP-GW-Client-Config' selected. A modal dialog box titled 'Configs' is open, showing the configuration details for 'GP-GW-Client-Config'. The 'Authentication Override' tab is selected, and the 'User/User Group' option is circled in orange. A yellow callout box points to this option with the text '本構成例では設定しない' (Not configured in this example). Other settings in the dialog include 'Name' (GP-GW-Client-Config), 'Generate cookie for authentication override' (unchecked), 'Accept cookie for authentication override' (unchecked), 'Cookie Lifetime' (Hours, 24), and 'Certificate to Encrypt/Decrypt Cookie' (None). 'OK' and 'Cancel' buttons are visible at the bottom of the dialog.

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings
Timeout

Configs

GP-GW-Client-Config

Authn Override User/User Group Network Settings

Retrieve Framed-IP-Address attribute from authentication server

No direct access to local network
No direct access to local network is applicable to Windows and Mac only

Authentication Server IP Pool ▲

Enter IP subnets or ranges (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100) to match the Framed IP attribute of the authentication server.

+ Add - Delete

These IPs will be added to the firewall's routing table

IP Pool

192.168.1.201-192.168.1.210

+ Add - Delete

These routes will be added to the client's routing table

Access Route ▲

Enter subnets need to be accessed by clients (e.g. 172.16.1.0/24)

+ Add - Delete

These routes will be added to the client's routing table

OK Cancel

GlobalProtect クライアントに割り当てる IP アドレス範囲

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The screenshot shows the 'GlobalProtect Gateway Configuration' dialog box. The 'Agent' tab is selected, and 'Satellite' is chosen. The 'HIP Notification' tab is also visible and circled in orange. A green callout bubble points to the 'HIP Notification' tab with the text '本構成例では設定しない' (Not configured in this example). The 'Inheritance Source' is set to 'None'. The 'Primary DNS' is set to '192.168.1.1', 'Secondary DNS' is 'None', 'Primary WINS' is 'None', and 'Secondary WINS' is 'None'. The 'DNS Suffix' is set to 'pppoelab.local'. There is an unchecked checkbox for 'Inherit DNS Suffixes'. 'OK' and 'Cancel' buttons are at the bottom right.

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

GlobalProtect ゲートウェイ 設定

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

GlobalProtect Gateway Configuration

General

Name: GP-Internal-GW

Authentication

Agent

Satellite

Network Settings

Interface: ethernet1/3

IP Address: 192.168.1.1/24

OK Cancel

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

GlobalProtect ゲートウェイ 設定

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

The screenshot shows the 'GlobalProtect Gateway Configuration' window with the 'Authentication' tab selected. The 'Server Authentication' section has 'SSL/TLS Service Profile' set to 'For-GP-Int-GW'. The 'Client Authentication' section contains a table with one entry: 'GP-Client-Auth' with OS 'Any', Authentication Profile 'Auth-Profile-for-GP', and Authentication Message 'Enter login credentials'. The 'Certificate Profile' is set to 'None'. The window includes 'Add', 'Delete', 'Clone', 'Move Up', and 'Move Down' buttons at the bottom of the table area, and 'OK' and 'Cancel' buttons at the bottom right.

<input type="checkbox"/>	Name	OS	Authentication Profile	Authentication Message
<input checked="" type="checkbox"/>	GP-Client-Auth	Any	Auth-Profile-for-GP	Enter login credentials

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

GlobalProtect ゲートウェイ 設定

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

GlobalProtect Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings | Timeout Settings | Client Settings | Network Services | HIP Notification

Tunnel Mode

Tunnel Interface: None

Max User: [1 - 25]

Enable IPSec

GlobalProtect IPSec Crypto: default

Enable X-Auth Support

Group Name: _____

Group Password: _____

Confirm Group Password: _____

Skip Auth on IKE Rekey









OK Cancel


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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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	

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

Dynamic IP Interface Status

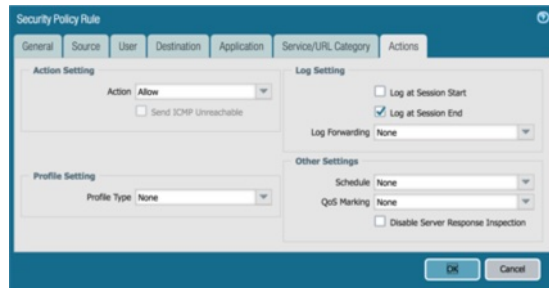
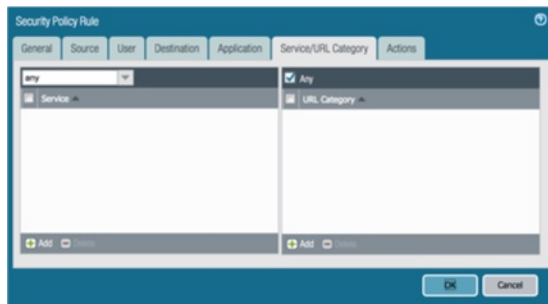
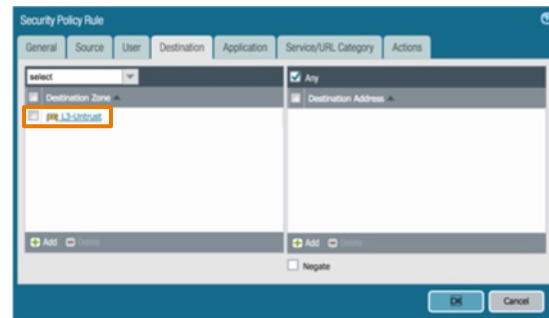
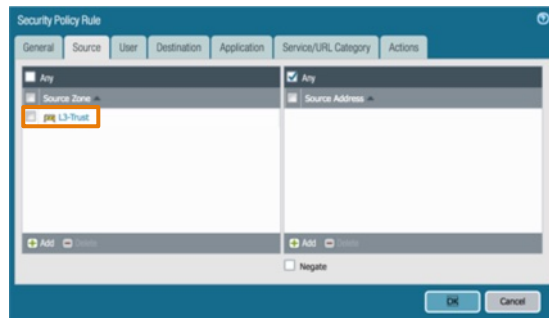
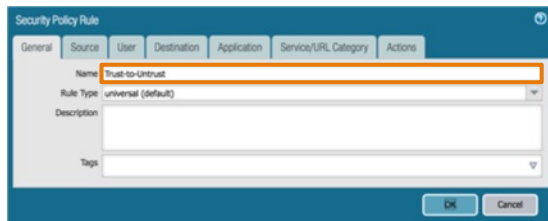
Interface ethernet1/1
Local IP Address 203.0.113.8
 Primary DNS 8.8.8.8
 Secondary DNS 8.8.4.4
 Primary WINS 0.0.0.0
 Secondary WINS 0.0.0.0
Remote IP Address 192.0.2.254
 PPPoE State Connected
 PPP State Connected
 Access Concentrator lab_pppoe_server
 AC MAC 00:0c:29:9f:b9:b9
 Authentication Method CHAP
 Passive mode Disabled
 Link MTU 1454

Connect Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

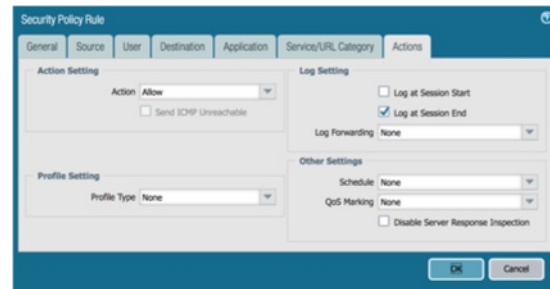
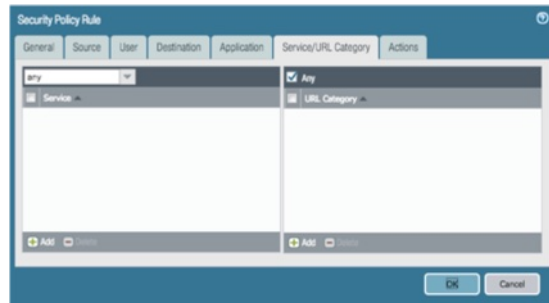
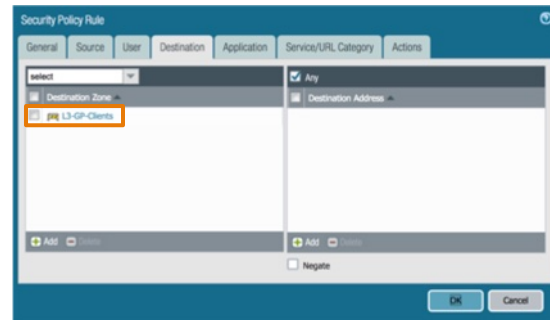
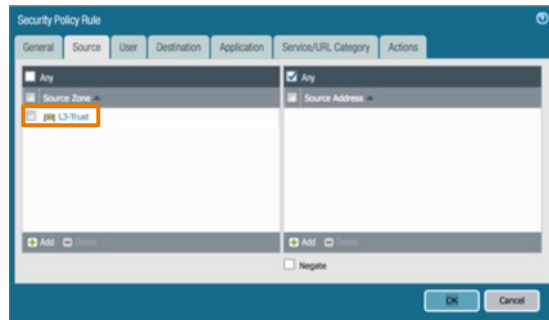
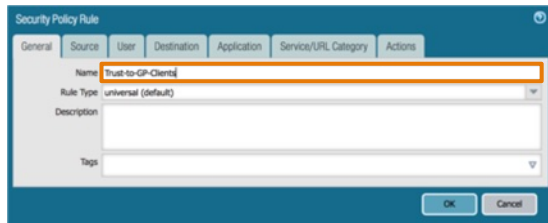
- インターネット向け通信用セキュリティポリシーの設定 (Policies > Security > Add)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

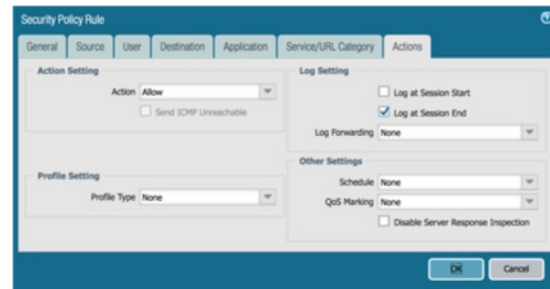
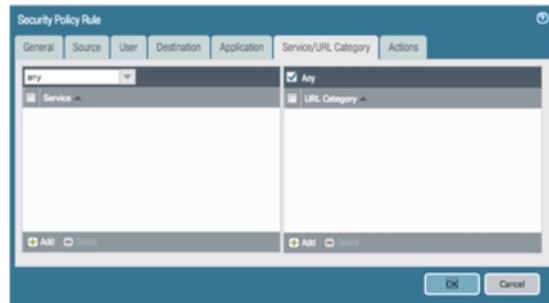
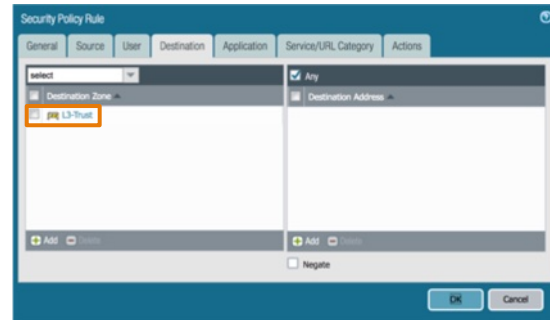
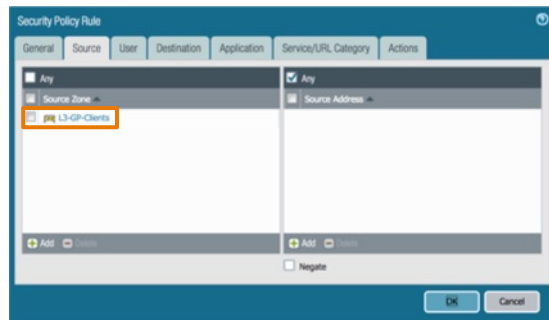
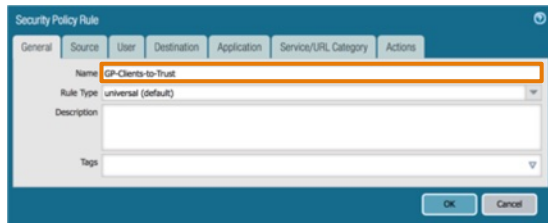
- 内部→GPクライアント通信用セキュリティポリシーの設定 (Policies > Security > Add)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

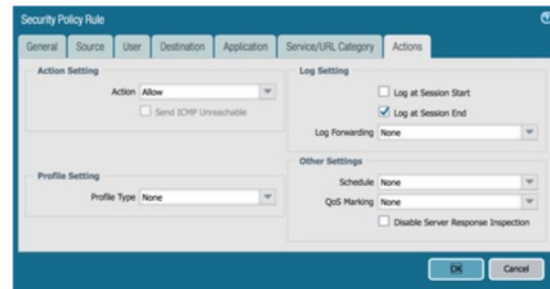
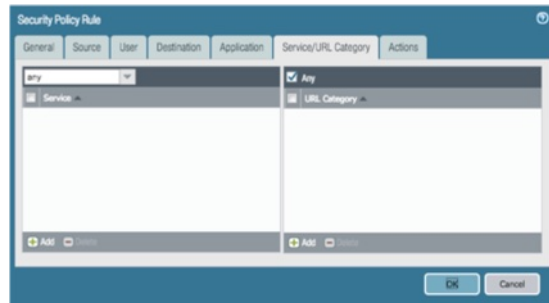
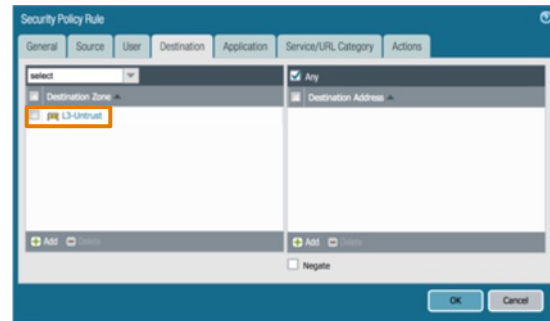
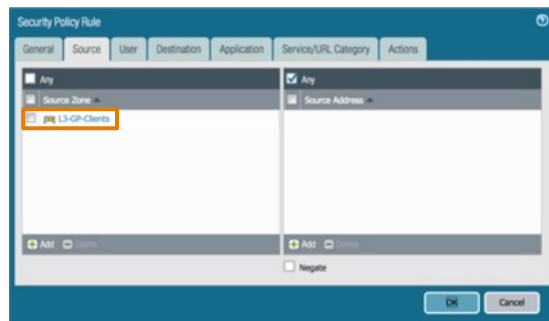
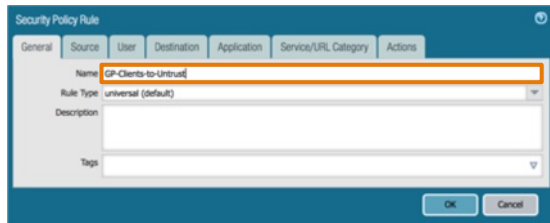
- GPクライアント→内部通信用セキュリティポリシーの設定 (Policies > Security > Add)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

	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	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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

NATポリシー設定

- 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)

させない

NAT Policy Rule configuration - General tab. The Name field is set to "No NAT". The NAT Type is set to "ipv4".

NAT Policy Rule configuration - Translated Packet tab. The Translation Type is set to "None".

NAT Policy Rule configuration - Original Packet tab. The Destination Zone is set to "L3-Untrust". The Source Zone is set to "L3-GP-Clients". The Destination Address is set to "203.0.113.8".

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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 Policy Rule configuration window, General tab. The Name field is set to "N to 1 NAT". The Description field is empty. The Tags field is empty. The NAT Type is set to "IPv4".

NAT Policy Rule configuration window, Translated Packet tab. The Source Address Translation section is active. The Translation Type is set to "Dynamic IP And Port". The Address Type is set to "Interface Address". The Interface is set to "ethernet1/1". The IP Address is set to "None". The Destination Address Translation section is inactive.

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 Policy Rule configuration window, Original Packet tab. The Destination Zone is set to "L3-Untrust". The Source Zone is set to "Any". The Source Address is set to "Any". The Destination Address is set to "Any". The Destination Interface is set to "any". The Service is set to "any".

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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	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

設定例 1

設定例 2

設定例 3

設定例 4

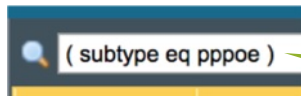
設定例 5

設定例 6

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@pppoeab.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@pppoeab.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

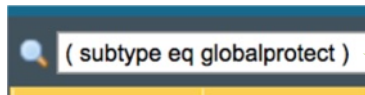
設定後のGlobalProtect 接続ログ例

- 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

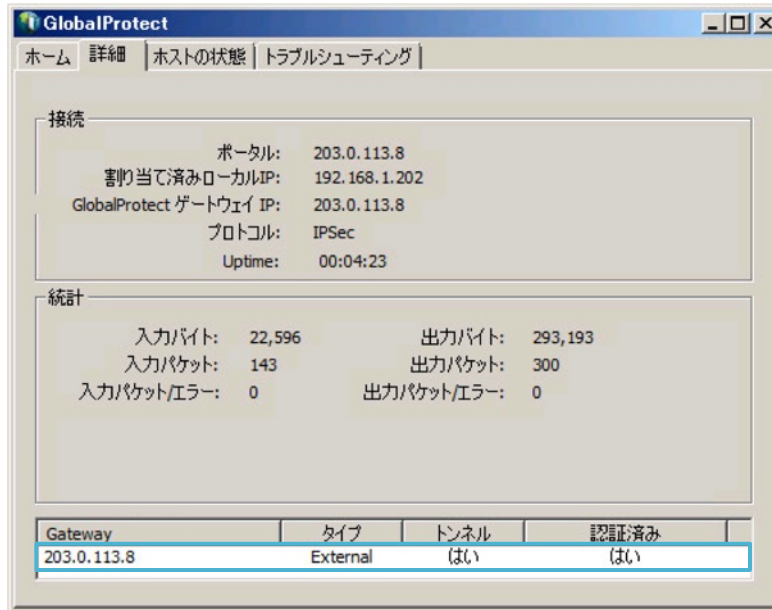
Receive Time	Type	Severity	Event	Object	Description
03/27 17:27:32	globalprotect	informational	globalprotectgateway-logout-succ	GP-External-GW-N	GlobalProtect gateway user logout succeeded. User name: GPuser01, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, Reason: client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



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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.

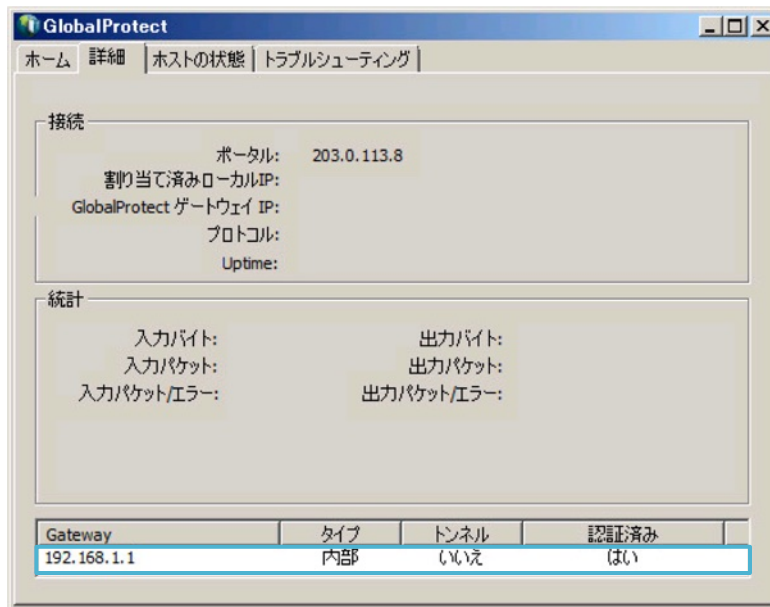
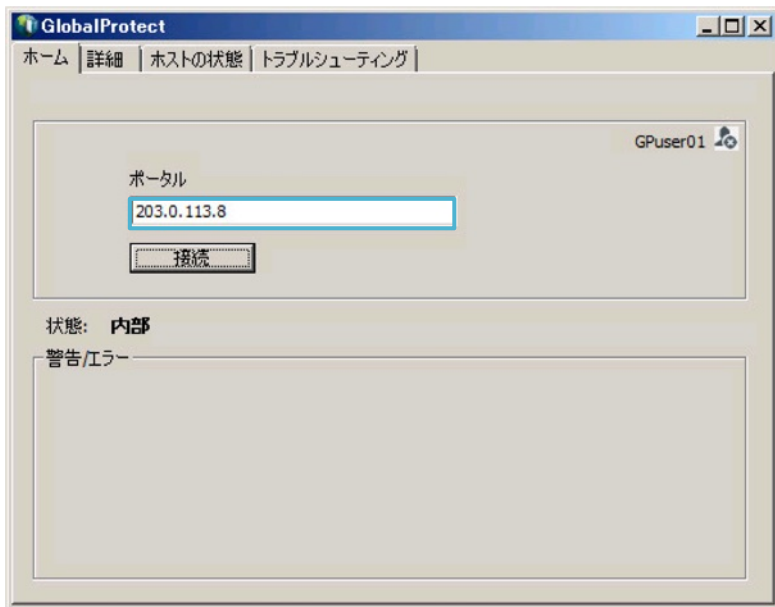


表示フィルタを使用することで必要なログを素早く確認することが可能

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 21775 Action allow Action Source from-policy Application ssl Rule Trust-to-Untrust Session End Reason tcp-rst-from-client Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/27 17:58:22 Start Time 2018/03/27 17:56:52 Receive Time 2018/03/27 17:58:22 Elapsed Time(sec) 60	User Address 192.168.1.103 Country 192.168.0.0-192.168.2... Port 50679 Zone L3-Trust Interface ethernet1/3 NAT IP 203.0.113.8 NAT Port 46541	User Address 111.221.29.253 Country Hong Kong Port 443 Zone L3-Untrust Interface ethernet1/1 NAT IP 111.221.29.253 NAT Port 443
	Details	Flags
	Bytes 6199 Bytes Received 4580 Bytes Sent 1619 Repeat Count 1 Packets 16 Packets Received 7 Packets Sent 9	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>


PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/27 17:58:22	end	ssl	allow	Trust-to-Untrust	6199	any

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 17492 Action allow Action Source from-policy Application ssh Rule GP-Clients-to-Trust Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/27 09:27:03 Start Time 2018/03/27 09:22:50 Receive Time 2018/03/27 09:27:03 Elapsed Time(sec) 238	User gpuser01 Address 192.168.1.201 Country 192.168.0.0-192.168.2... Port 49306 Zone L3-GP-Clients Interface tunnel	User Address 192.168.1.101 Country 192.168.0.0-192.168.2... Port 22 Zone L3-Trust Interface ethernet1/3
	Details	Flags
	Bytes 33521 Bytes Received 18315 Bytes Sent 15206 Repeat Count 1 Packets 200 Packets Received 94 Packets Sent 106	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/27 09:27:03	end	ssh	allow	GP-Clients-to-Trust	33521	any

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



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

Detailed Log View

General	Source	Destination
Session ID 21541 Action allow Action Source from-policy Application ms-update Rule GP-Clients-to-Untrust Session End Reason tcp-rst-from-server Category computer-and-internet-info Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/27 17:25:06 Start Time 2018/03/27 17:22:50 Receive Time 2018/03/27 17:25:06 Elapsed Time(sec) 105	User gpuser01 Address 192.168.1.202 Country 192.168.0.0-192.168.2... Port 49177 Zone L3-GP-Clients Interface tunnel NAT IP 203.0.113.8 NAT Port 12539	User Address 191.234.72.188 Country United States Port 443 Zone L3-Untrust Interface ethernet1/1 NAT IP 191.234.72.188 NAT Port 443
	Details	Flags
	Bytes 301603 Bytes Received 18037 Bytes Sent 283566 Repeat Count 1 Packets 330 Packets Received 113 Packets Sent 217	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/27 17:25:06	end	ms-update	allow	GP-Clients-to-Untrust	301603	computer-and-internet-info

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 17558 Action allow Action Source from-policy Application ping Rule Trust-to-GP-Clients Session End Reason aged-out Category any Virtual System Device SN IP Protocol icmp Log Action Generated Time 2018/03/27 09:26:42 Start Time 2018/03/27 09:26:30 Receive Time 2018/03/27 09:26:42 Elapsed Time(sec) 0	User Address 192.168.1.101 Country 192.168.0.0-192.168.2... Port 0 Zone L3-Trust Interface ethernet1/3	User gpuser01 Address 192.168.1.201 Country 192.168.0.0-192.168.2... Port 0 Zone L3-GP-Clients Interface tunnel

Details	Flags
Bytes 816 Bytes Received 424 Bytes Sent 392 Repeat Count 4 Packets 8 Packets Received 4 Packets Sent 4	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/27 09:26:42	end	ping	allow	Trust-to-GP-Clients	816	any

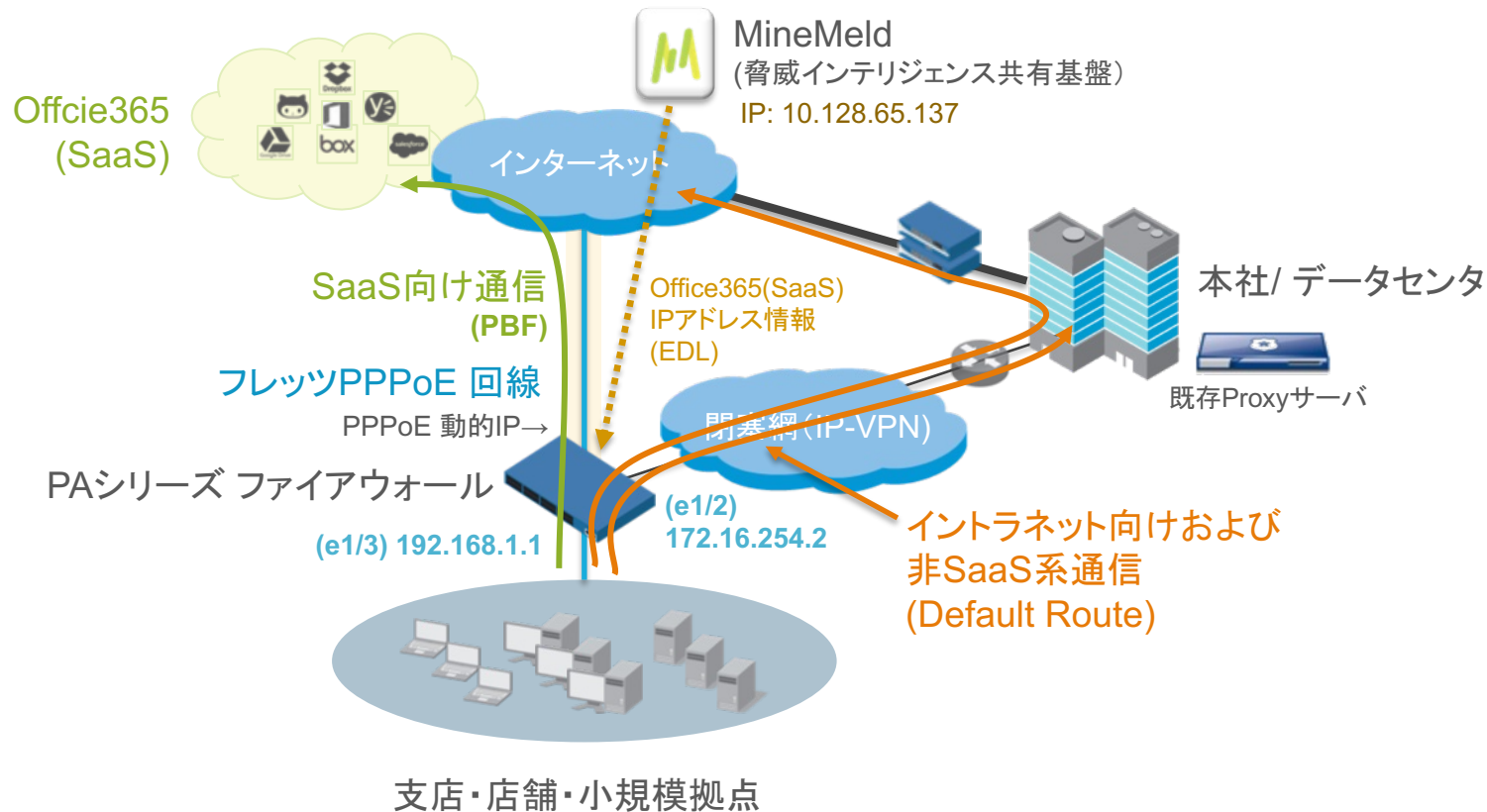
Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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:



- 設定例 1
- 設定例 2
- 設定例 3
- 設定例 4
- 設定例 5
- 設定例 6



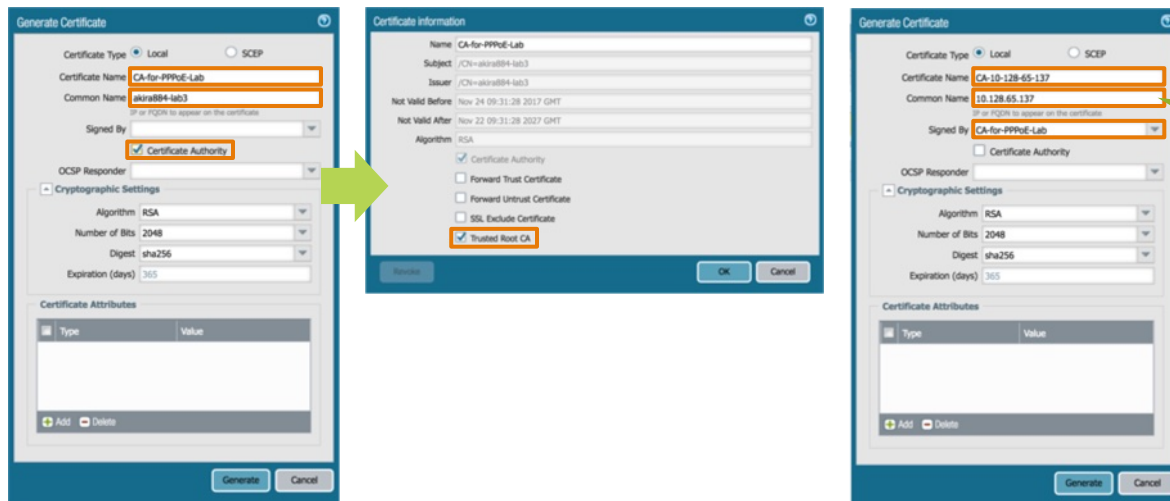
コンフィグレーションに関するポイント・留意事項

項目	内容
PPPoE 関連	<ul style="list-style-type: none">・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す。
その他	<ul style="list-style-type: none">・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) <p>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</p> <ul style="list-style-type: none">・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)



MineMeld が稼働している
サーバのIPアドレス(例)

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

Name	Subject	Issuer	CA	K...	Expires	Sta...	Al...	Usage
CA-for-PPPoE-Lab	CN = akira884-lab3	CN = akira884-lab3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Nov 22 09:34:25 2027 GMT	valid	RSA	

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)

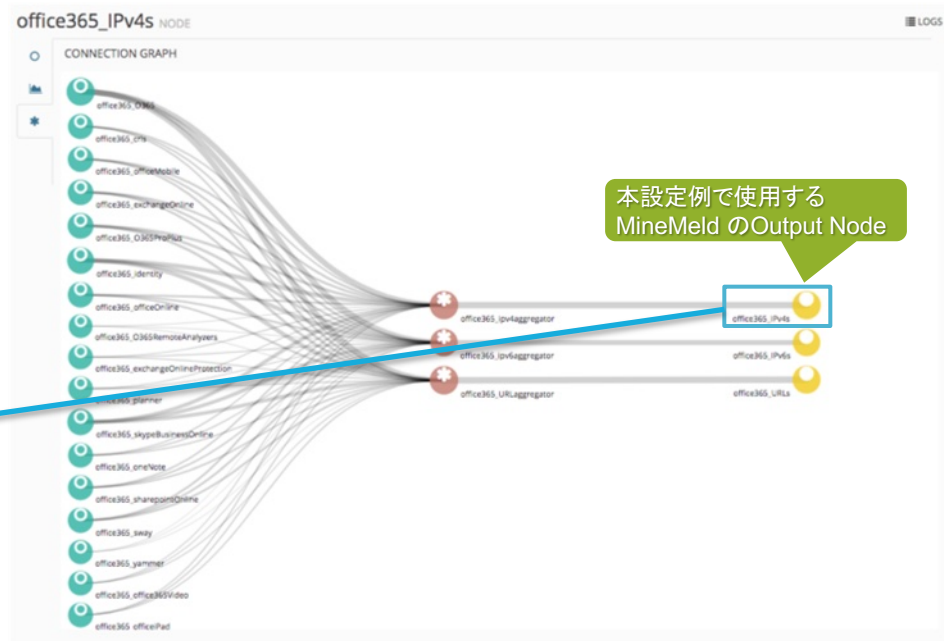


office365_IPv4s NODE

STATUS

CLASS	minemeld.ft.redis.RedisSet
PROTOTYPE	stdlib.feedHCWithValue
STATE	STARTED
FEED BASE URL	https://10.128.65.137/feeds/office365_IPv4s
TAGS	
# INDICATORS	588

PA のEDL(外部ダイナミックリスト) 設定でしているURL



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

External Dynamic Lists

Name: Office365-IPv4s

Type: IP List

Description:

Source: https://10.128.65.137/feeds/office365_IPv4s

Repeat: Five Minute

Test Source URL OK Cancel

MineMeld が稼働している
サーバのIPアドレス(例)

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)

Interface Management Profile

Name: ping-only

Permitted Services

- Ping
- Telnet
- SSH
- HTTP
- HTTP OCSP
- HTTPS
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

Permitted IP Addresses

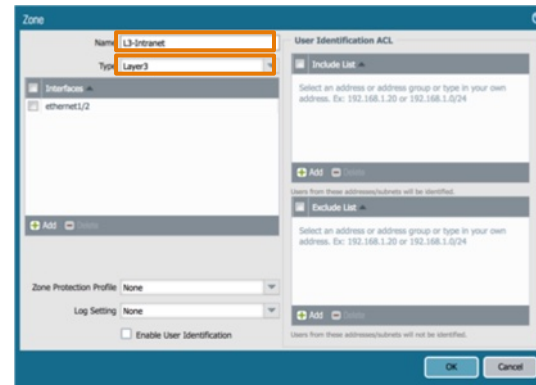
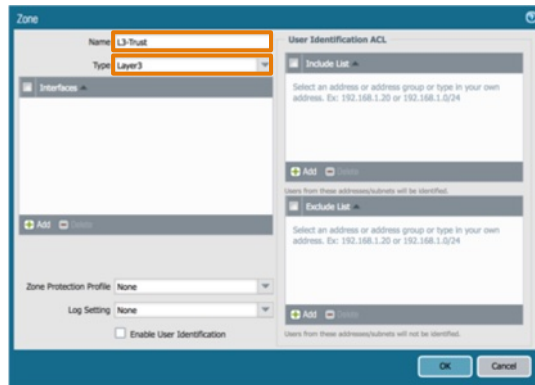
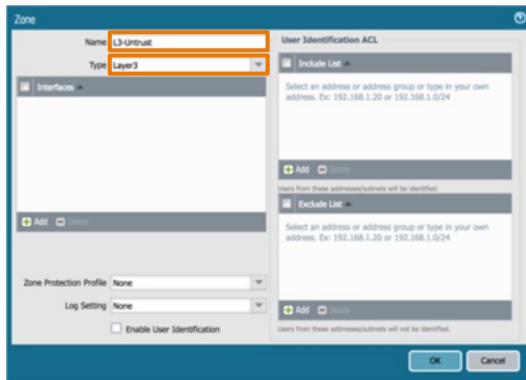
+ Add - Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

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트라ネット用セキュリティゾーンを作成 (Network > Zones)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Trust'. The 'Config' tab is active, with sub-tabs for 'IPv4', 'IPv6', and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Config' tab is selected, and the 'IPV4' sub-tab is active. Under the 'Type' section, 'Static' is selected. A table of IP addresses is shown with '192.168.1.1/24' highlighted. The 'Add', 'Delete', 'Move Up', and 'Move Down' buttons are visible at the bottom of the table. The 'OK' and 'Cancel' buttons are at the bottom right of the window.

Ethernet Interface

Interface Name: ethernet1/3

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPV4 | IPV6 | Advanced

Type: Static PPPoE DHCP Client

IP
<input checked="" type="checkbox"/> 192.168.1.1/24

+ Add - Delete ↕ Move Up ↕ Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

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)

Ethernet Interface

Interface Name: ethernet1/3

Comment: []

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Untrust'. The 'Config' tab is active, with sub-tabs for 'IPv4' and 'Advanced'. 'OK' and 'Cancel' buttons are at the bottom right.

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
Config	IPv4 Advanced
Assign Interface To	
Virtual Router	default
Security Zone	L3-Untrust

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)

Ethernet Interface

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 Advanced

Type Static PPPoE DHCP Client

General Advanced

Enable

Username dyn-ip-user101@pppoelab.local

Password *****

Confirm Password *****

Show PPPoE Client Runtime Info

OK Cancel

PPPoE を選択

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)

Ethernet Interface

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 Advanced

Type Static PPPoE DHCP Client

General Advanced

Authentication auto

Static Address None

automatically create default route pointing to peer

Default Route Metric [1 - 65535]

Access Concentrator

Service

Passive

OK Cancel

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)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: 1454

Untagged Subinterface

OK | Cancel

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)

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/2'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is 'None'. The 'Assign Interface To' section is expanded, showing 'Virtual Router' set to 'default' and 'Security Zone' set to 'L3-Intranet'. The 'Config' tab is selected, and the 'OK' and 'Cancel' buttons are visible at the bottom.

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)

The screenshot shows the configuration window for an Ethernet Interface. The interface name is 'ethernet1/2'. The interface type is 'Layer3'. The netflow profile is 'None'. The configuration is set to 'Static' type. A table of IP addresses is shown with '172.16.254.2/24' highlighted. The interface also shows 'Add', 'Delete', 'Move Up', and 'Move Down' buttons. The IP address/netmask example is '192.168.2.254/24'.

IP
172.16.254.2/24

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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)

Ethernet Interface

Interface Name: ethernet1/2

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Link Settings

Link Speed: auto | Link Duplex: auto | Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP

Management Profile: ping-only

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60








Untagged Subinterface

OK Cancel

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	

Dynamic IP Interface Status

Interface ethernet1/1

Local IP Address 198.51.100.101

Primary DNS 8.8.8.8

Secondary DNS 8.8.4.4

Primary WINS 0.0.0.0

Secondary WINS 0.0.0.0

Remote IP Address 192.0.2.254

PPPoE State Connected

PPP State Connected

Access Concentrator lab_pppoe_server

AC MAC 00:0c:29:9f:b9:b9

Authentication Method CHAP

Passive mode Disabled

Link MTU 1454

Connect Close

設定例 1

設定例 2

設定例 3

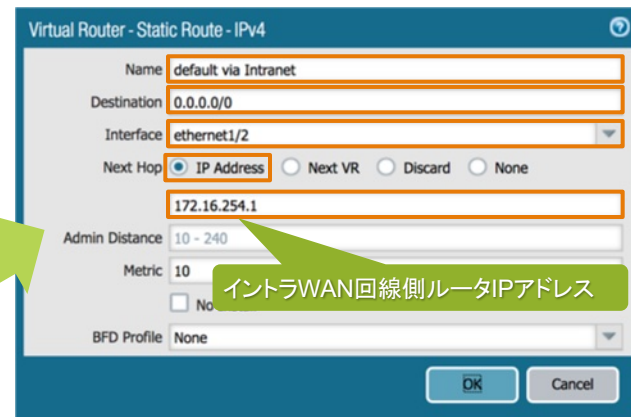
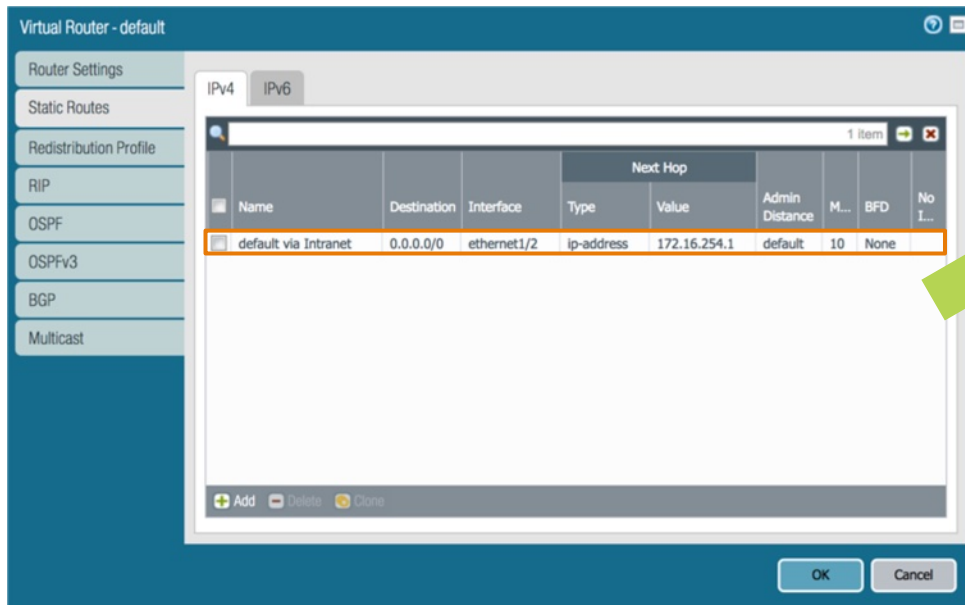
設定例 4

設定例 5

設定例 6

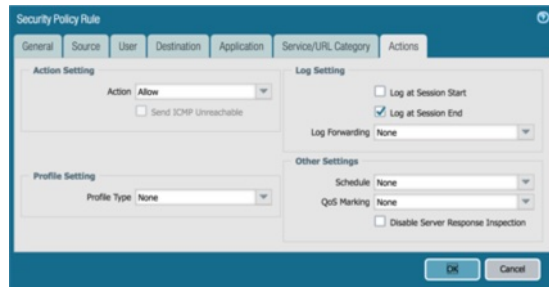
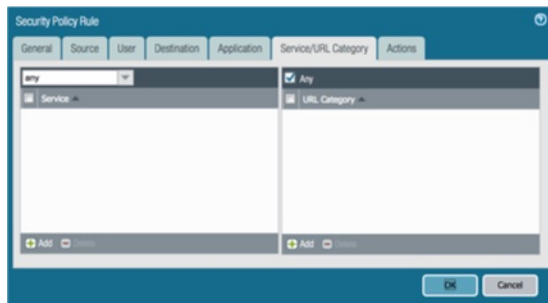
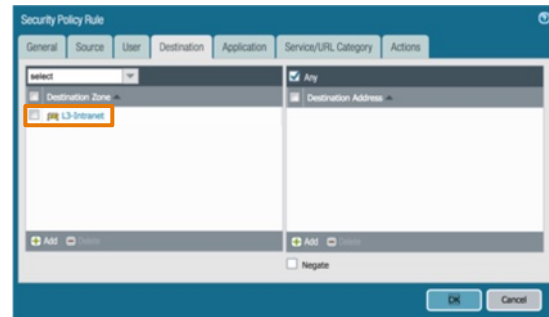
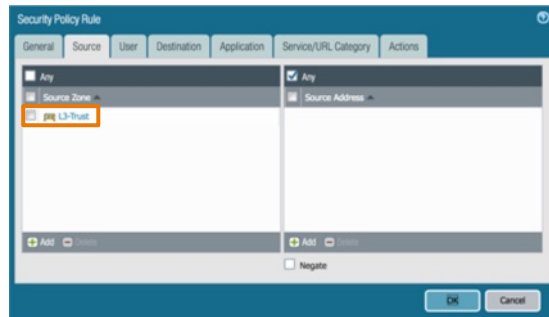
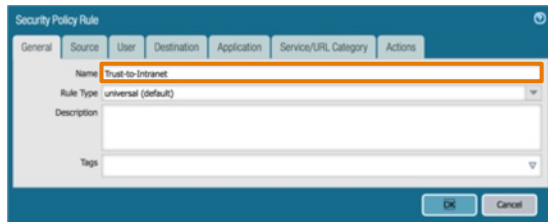
イントラネット向けルーティング設定

- 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

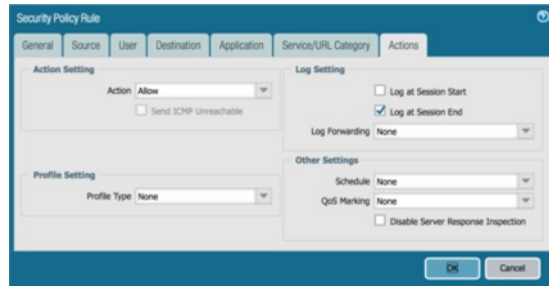
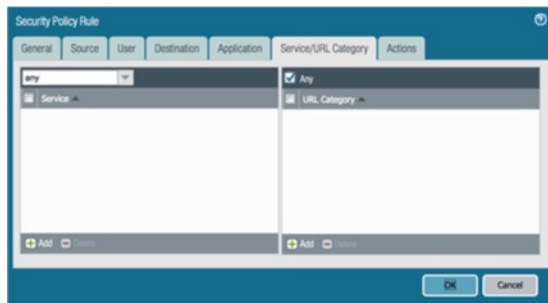
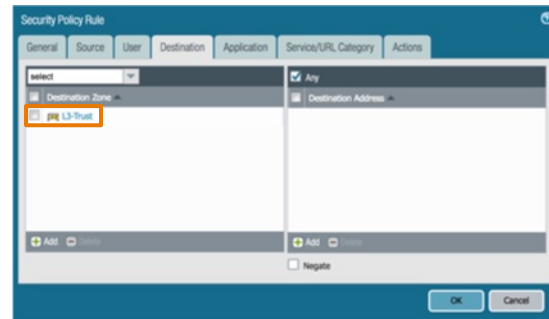
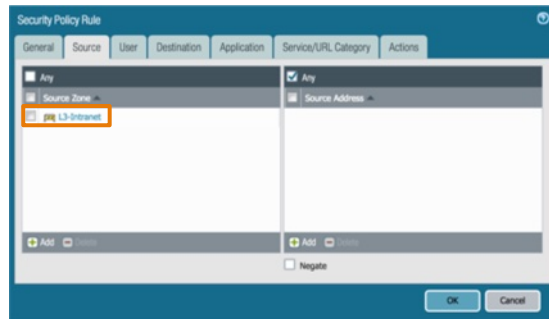
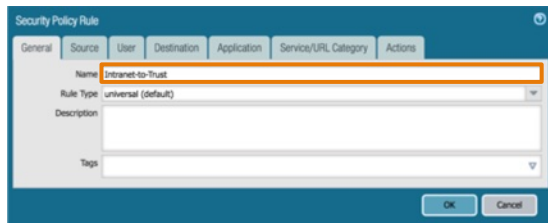
- 内部→イントラネット向け通信用セキュリティポリシーの設定 (Policies > Security > Add)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

セキュリティポリシー設定

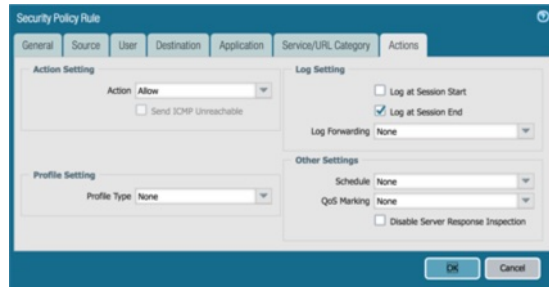
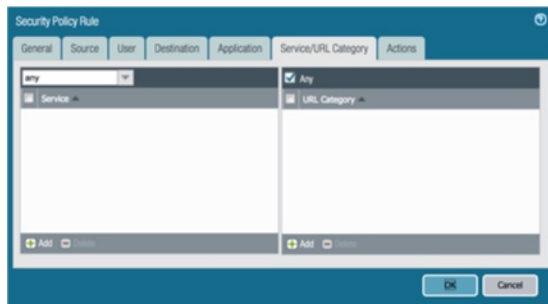
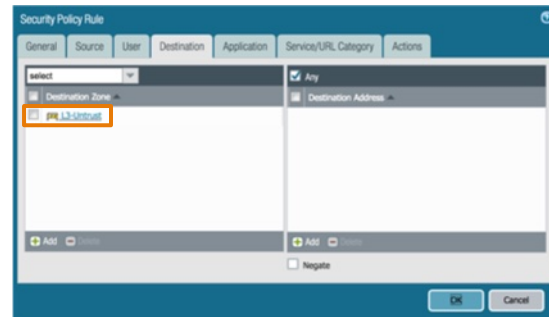
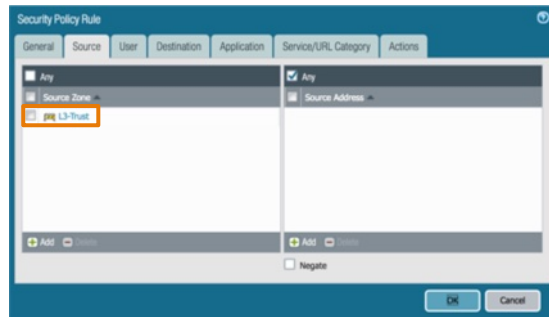
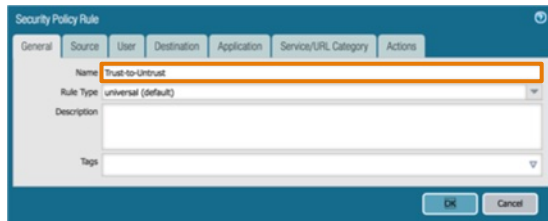
- イントラネット→内部向け通信用セキュリティポリシーの設定 (Policies > Security > Add)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)

	Name	Tags	Type	Source			Destination		Application	Service	Action	Profile	Options
				Zone	Address	User	Zone	Address					
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

設定例 1

設定例 2

設定例 3

設定例 4

設定例 5

設定例 6

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 Policy Rule

General Original Packet Translated Packet

Name N to 1 NAT

Description

Tags

NAT Type IPv4

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type Dynamic IP And Port

Address Type Interface Address

Interface ethernet1/1

IP Address None

Destination Address Translation

Translated Address

Translated Port [1 - 65535]

OK Cancel

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

NAT Policy Rule

General Original Packet Translated Packet

Any

Source Zone L3-Untrust

Destination Zone L3-Trust

Destination Interface any

Service any

Any

Source Address

Destination Address

Add Delete

OK Cancel

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)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

NATポリシー設定一覧

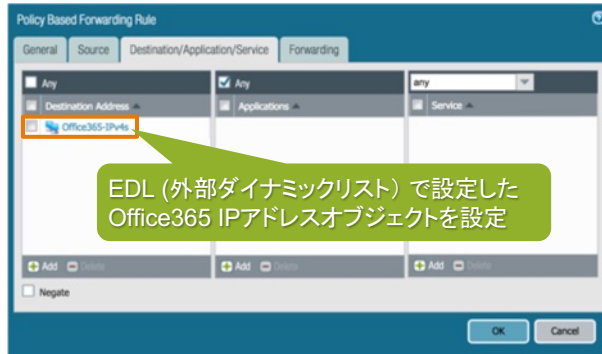
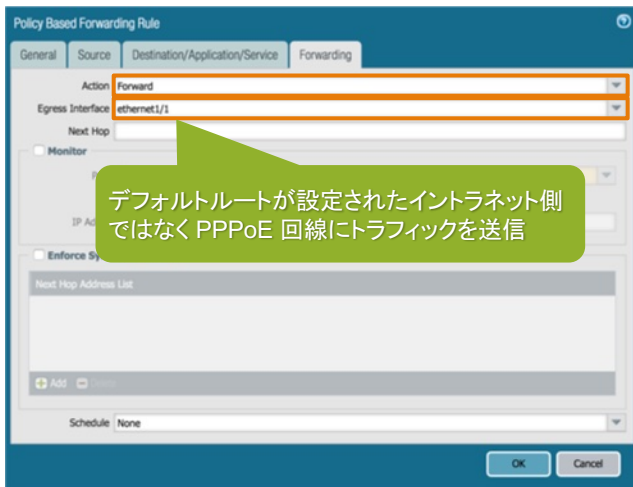
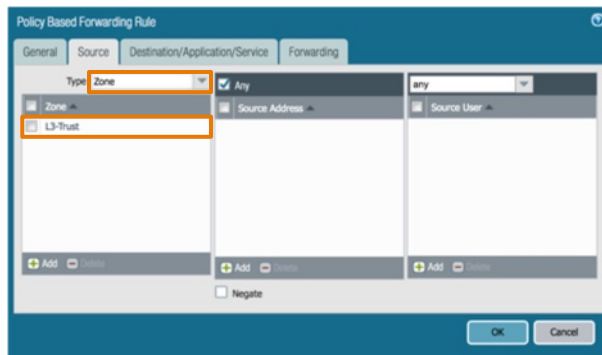
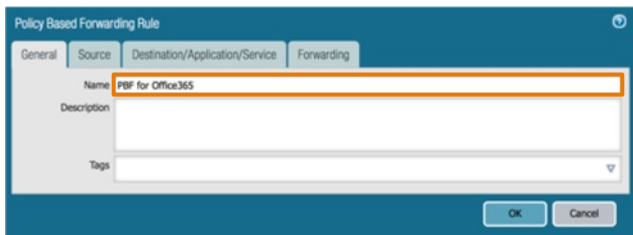
- NATポリシー設定一覧 (Policies > NAT)

	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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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)



設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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 Based Forwarding)

Name	Tags	Source			Destination		Application	Service	Action	Forwarding			Monitoring			Schedule
		Zone/Interface	Address	User	Address	Egress I/F				Next Hop	Enforce Symmetric Return	Profile	Target	Disable If Unreachable		
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)

Virtual Router - default

Routing | RIP | OSPF | OSPFv3 | BGP | Multicast | BFD Summary Information

Route Table | Forwarding Table

Destination	Next Hop	Metric	Flags	Interface
0.0.0.0/0	172.16.254.1	10	A S	ethernet1/2
172.16.254.0/24	172.16.254.2	0	A C	ethernet1/2
172.16.254.2/32	0.0.0.0	0	A H	
192.0.2.254/32	198.51.100.101	10	A S	ethernet1/1
192.168.1.0/24	192.168.1.1	0	A C	ethernet1/3
192.168.1.1/32	0.0.0.0	0	A H	
198.51.100.101/32	0.0.0.0	0	A H	

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)

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 3648 Action allow Action Source from-policy Application dns Rule Trust-to-Intranet Session End Reason aged-out Category any Virtual System Device SN IP Protocol udp Log Action Generated Time 2018/03/28 16:12:30 Start Time 2018/03/28 16:12:00 Receive Time 2018/03/28 16:12:30 Elapsed Time(sec) 0	User Address 192.168.1.103 Country 192.168.0.0-192.168.2... Port 54464 Zone L3-Trust Interface ethernet1/3	User Address 8.8.8.8 Country United States Port 53 Zone L3-Intranet Interface ethernet1/2

Details	Flags
Bytes 385 Bytes Received 304 Bytes Sent 81 Repeat Count 1 Packets 2 Packets Received 1 Packets Sent 1	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>


PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/28 16:12:30	end	dns	allow	Trust-to-Intranet	385	any

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 3665 Action allow Action Source from-policy Application ssh Rule Intranet-to-Trust Session End Reason tcp-fin Category any Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/28 16:21:36 Start Time 2018/03/28 16:21:10 Receive Time 2018/03/28 16:21:36 Elapsed Time(sec) 10	User Address 172.16.254.1 Country 172.16.0.0-172.31.255... Port 46762 Zone L3-Intranet Interface ethernet1/2	User Address 192.168.1.101 Country 192.168.0.0-192.168.2... Port 22 Zone L3-Trust Interface ethernet1/3

Details	Flags
Bytes 13074 Bytes Received 6237 Bytes Sent 6837 Repeat Count 1 Packets 92 Packets Received 38 Packets Sent 54	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Category
	2018/03/28 16:21:36	end	ssh	allow	Intranet-to-Trust	13074	any

Close

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6

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

Detailed Log View

General	Source	Destination
Session ID 2800 Action allow Action Source from-policy Application ms-office365-base Rule Trust-to-Untrust Session End Reason tcp-rst-from-server Category computer-and-internet-info Virtual System Device SN IP Protocol tcp Log Action Generated Time 2018/03/28 13:34:41 Start Time 2018/03/28 13:32:37 Receive Time 2018/03/28 13:34:41 Elapsed Time(sec) 109	User Address 192.168.1.103 Country 192.168.0.0-192.168.2... Port 49526 Zone L3-Trust Interface ethernet1/3 NAT IP 198.51.100.101 NAT Port 30525	User Address 23.100.88.32 Country Hong Kong Port 443 Zone L3-Untrust Interface ethernet1/1 NAT IP 23.100.88.32 NAT Port 443

Details

Bytes 5083
Bytes Received 4233
Bytes Sent 850
Repeat Count 1
Packets 14
Packets Received 6
Packets Sent 8

Flags

Captive Portal	<input type="checkbox"/>
Proxy Transaction	<input type="checkbox"/>
Decrypted	<input type="checkbox"/>
Packet Capture	<input type="checkbox"/>
Client to Server	<input checked="" type="checkbox"/>
Server to Client	<input type="checkbox"/>
Symmetric Return	<input type="checkbox"/>
Mirrored	<input type="checkbox"/>

PCAP Receive Time Type Application Action Rule Bytes Category

2018/03/28 13:34:41	end	ms-office365-base	allow	Trust-to-Untrust	5083	computer-and-internet-info
---------------------	-----	-------------------	-------	------------------	------	----------------------------

Close

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

設定例 1
設定例 2
設定例 3
設定例 4
設定例 5
設定例 6



paloalto
NETWORKS®