



# Mist 設定マニュアル - WAN Assurance - WAN Edge の設定 Application Policy の設定

---

ジュニパーネットワークス株式会社  
2024年12月 Ver 1.0

# はじめに

- ❖ 本マニュアルは、『WAN Edge の設定 Application Policy の設定』について説明します
- ❖ 手順内容は 2024年12月 時点の Mist Cloud にて確認を実施しております  
実際の画面と表示が異なる場合は以下のアップデート情報をご確認ください  
<https://www.mist.com/documentation/category/product-updates/>
- ❖ 設定内容やパラメータは導入する環境や構成によって異なります  
各種設定内容の詳細は下記リンクよりご確認ください  
<https://www.mist.com/documentation/>
- ❖ 他にも多数の Mist 日本語マニュアルを「ソリューション&テクニカル情報サイト」に掲載しております  
<https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html>
- ❖ **本資料の内容は資料作成時点におけるものであり事前の通告無しに内容を変更する場合があります**  
**また本資料に記載された構成や機能を提供することを条件として購入することはできません**

# テンプレートとサイト変数の活用

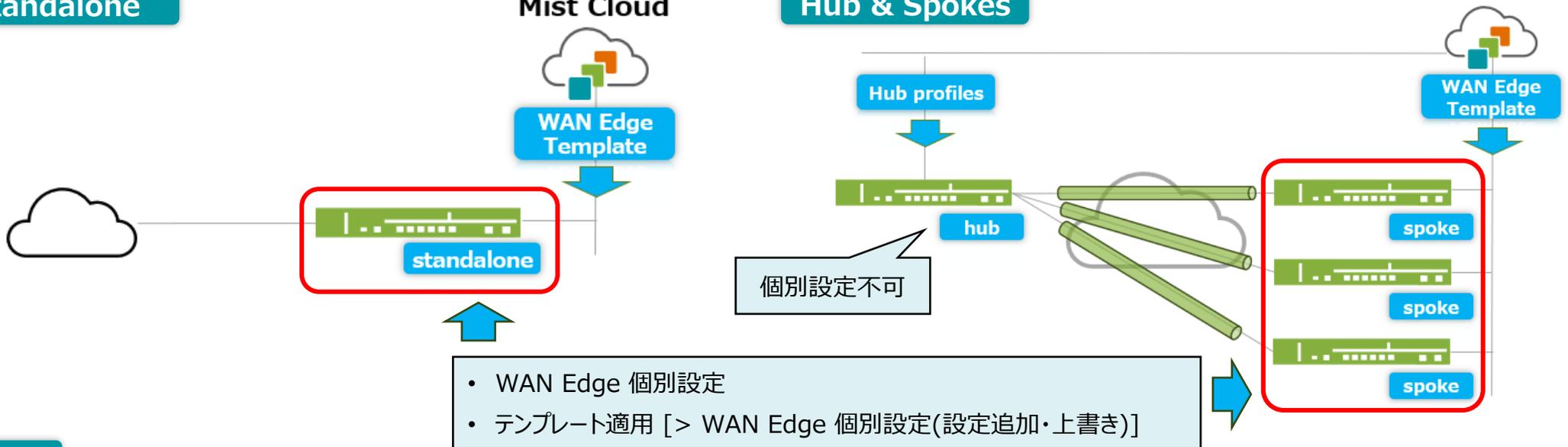
Template with Site Variables for agility, portability and scalability

Standalone

Mist Cloud

Hub & Spokes

Mist Cloud



## NOTE

- テンプレート、および、サイト変数の利用が推奨です
- WAN Edge 個別設定(テンプレートなし)、および、各テンプレート (Hub Profile・WAN Edge Template Standalone/Spoke) で設定できます
- WAN Edge Template Standalone/Spoke テンプレートを適用した WAN Edge 個別設定で、一部設定の追加や上書きができます
- テンプレート設定が上書きされている場合、その設定については、テンプレートを編集しても変更が適用されない(最終的に上書きされる)ため、上書き動作について十分に理解した上で利用する必要があります
- Hub Profile を適用した WAN Edge で設定の追加や上書き等の変更はできません
- WAN Edge 個別設定、および、テンプレート適用下での設定追加や上書きはテンプレートによる拡張性や敏捷性、可搬性が損なわれる可能性があるため、限定的な利用が推奨されます

# Application Policy の設定

## 機器選択

1. [WAN Edges] から [WAN Edges] をクリックします
2. [site] を選択し、設定する機器をクリックします

Juniper Mist™ MIST WAN ASSURANCE

1 WAN Edges site Primary Site List Topology

Change language (en) THU 13:44

Inventory Claim WAN Edges

100% Config Success 100% Version Compliance 100% WAN Edge Uptime

<input type="checkbox"/>	Name	Status	IP Address	Model	Version	Topology	Managed	Insights
<input type="checkbox"/>		Connected		SSR120	6.0.8-20	--		WAN Edge Insights

List: 表形式で表示  
Topology: トポロジー表示

# Application Policy の設定

## Override Template Settings

テンプレートを設定し適用している場合、WAN Edge に Application Policy が反映されています  
[Override Template Settings] にチェックを入れると、ポリシーの変更や追加が可能です

- [\[Import Application Policy\]](#) : Organization > Application Policy の設定を参照し、インポートします
- [\[Add Application Policy\]](#) : WAN Edge に個別の Application Policy を追加します

ポリシーを変更・追加する場合、クリックします

Organization > Application Policy に遷移します

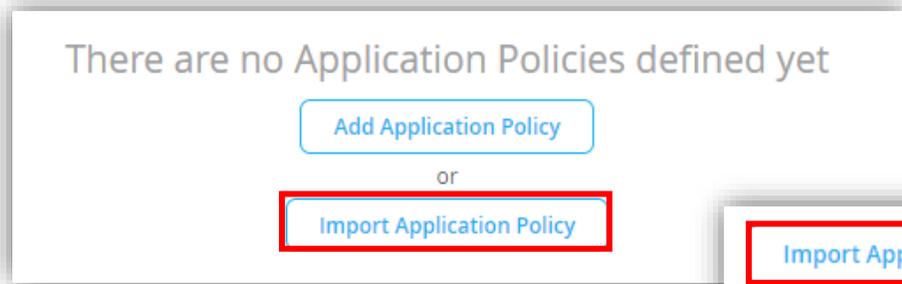
<input type="checkbox"/>	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP ⓘ	TRAFFIC STEERING
<input type="checkbox"/>	1	DMZ_OUT		+ DMZ ×	→ ✓ →	ANY × +	None ▾	underlay × ...
<input type="checkbox"/>	2	LAN_OUT		+ LAN ×	→ ✓ →	ANY × +	None ▾	underlay × ...
<input type="checkbox"/>	3	MGMT_OUT		+ MGMT ×	→ ✓ →	ANY × +	None ▾	underlay × ...

テンプレートで設定されたポリシーの変更もできます

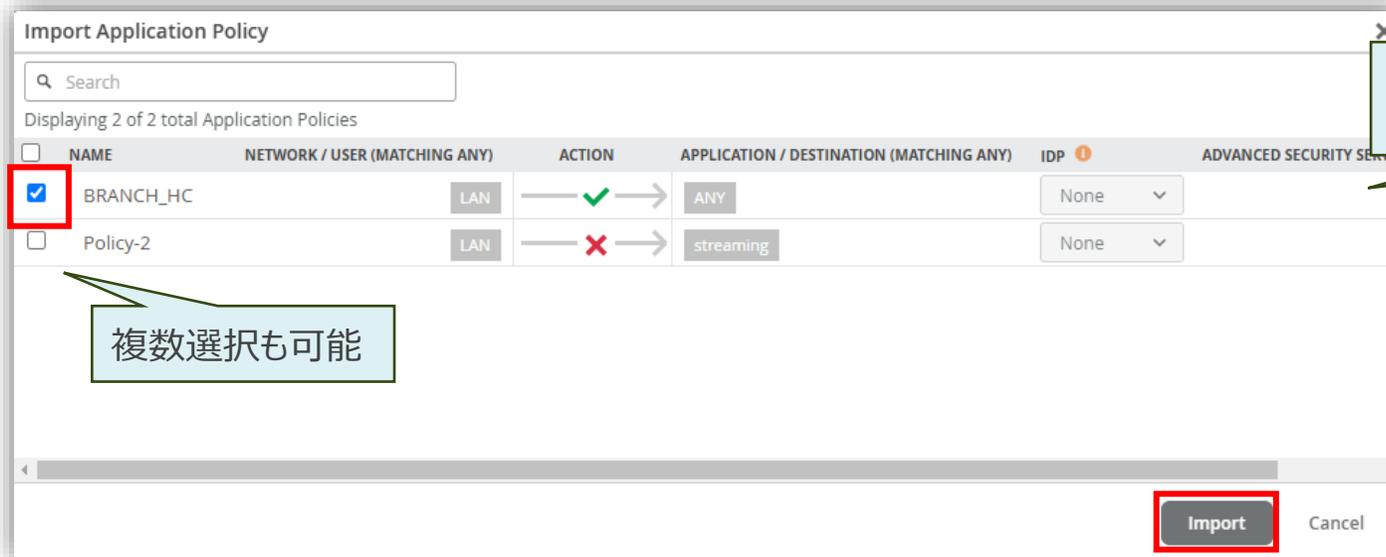
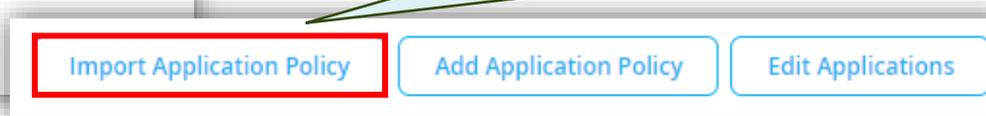
# Application Policy の設定

## Import Application Policy

1. [Import Application Policy] をクリックします
2. 事前に定義(Organization > Application Policy で設定) した Application Policy をチェックして、[Import] します



すでに作成済みの Application Policy がある場合は一覧の右上に表示されます



Organization > Application Policy で設定したポリシーから選択します

複数選択も可能

# Application Policy の設定

## Import Application Policy

3. [+] をクリックして、宛先パスとなる Traffic Steering を割り当てます  
複数設定する場合は、[Import Application Policy]、または、[Add Application Policy] で追加します

APPLICATION POLICIES ▲ ⚠ Destination zone in SRX is determined by the Traffic Steering path. Please ensure that policies have Traffic Steering assigned.

Search

Import Application Policy Add Application Policy Edit Applications

Displaying 1 of 1 total Application Policies

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP ⓘ	ADVANCED SECURITY SERVICES (SRX ONLY)	TRAFFIC STEERING
1	BRANCH_HC	✓	LAN	→ ✓ →	ANY	None	+	+

Template から Import した Policy には ✓ マークが付きま

Search

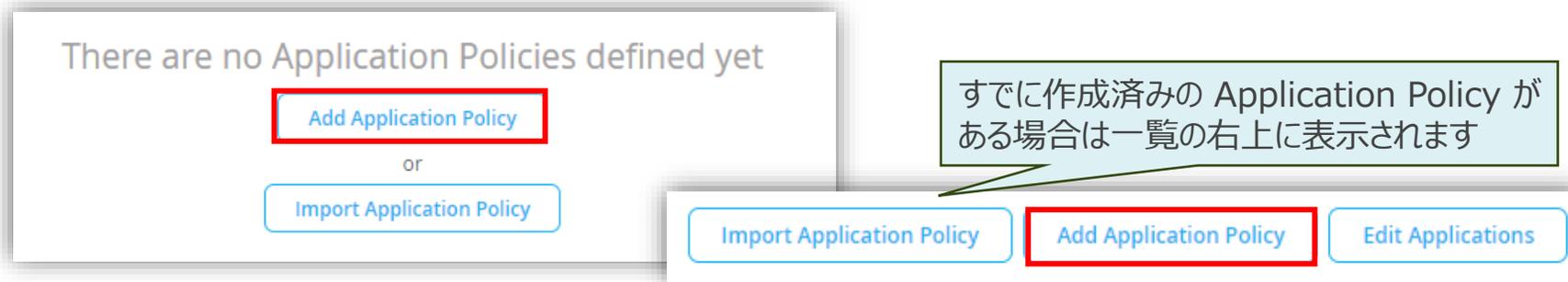
wan

Traffic Steering で設定したものを

# Application Policy の設定

## Add Application Policy

1. [Add Application Policy] をクリックします



# Application Policy の設定

## Add Application Policy

### 2. 各パラメータを設定します

1 2 3 4 5 6 7

NO. NAME ORG IMPORTED NETWORK / USER (MATCHING ANY) ACTION APPLICATION / DESTINATION (MATCHING ANY) IDP ADVANCED SECURITY SERVICES (SRX ONLY) TRAFFIC STEERING

1 Policy-1 + → + None + + ...

From(Src) To(Dst)

✓ Allow ✗ Block

1 クリックしてポリシー名 [Name] を変更します

2 [+ ] をクリック、予め作成した [NETWORK/USER] を選択します (複数選択可)

3 [Action] を選択します(Allow or Block)

4 [+ ] をクリック、[APPLICATION/DESTINATION] を選択します(複数選択可)  
予め作成した Application、または、事前定義済みの Built-In: any を選択

5 IDP プロファイルを選択します  
Built-in、または、例外を追加設定した Bypass Profile(要設定) を適用

6 ADVANCED SECURITY SERVICES(SRX Only) を設定します  
[+] をクリック、オプションを選択します

7 [+] をクリック、Traffic Steering を選択します

IDP/URL Filtering のライセンス購入が必要です

IDP Profiles	Descriptions
Critical Only - SRX	重要な攻撃シグネチャを検出し、推奨アクションを実行(SRXのみ)
Standard	エンタープライズ用標準シグネチャ(Juniper Recommended)
Strict	悪意のあるトラフィックによるリスクを最小限に抑えるため、接続のクローズ/ブロックを優先
Alert	アラートのみ、アクションなし
None	IDP 無効

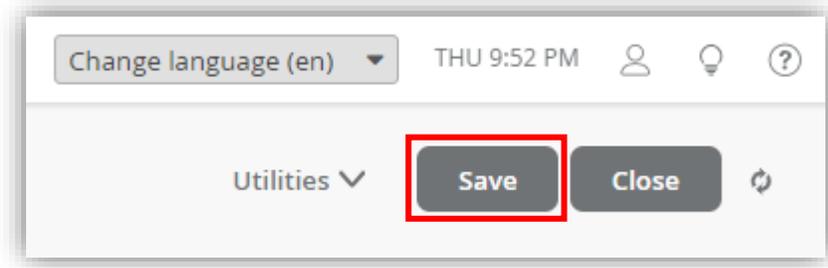
### NOTE

Network、Application、Traffic Steering 等は事前に設定しておく必要があります

# Application Policy の設定

## Application Policy

Application Policy 設定後、画面右上の [Save] をクリックして保存します





**Thank you**

**JUNIPER**  
NETWORKS®