



APAC Cohesion  
AI-Driven Enterprise / Connected Security  
(AIDE・CSEC)  
Tech Roundup Q2-2023

ジュニパーネットワークス株式会社

JUNIPER  
NETWORKS | Driven by  
Experience™



# Agenda

- AI ドリブン SD-WAN
- デモリアレンス
- ジュニパー SASE
- Mist Secure Edge 統合
- サマリー
- リソース

# 免責事項

この製品の方向性に関する声明は、ジュニパーネットワークスの現在の意図を示すものであり、予告なしにいつでも変更されることがあります。ジュニパーネットワークスが本ステートメントに記載された特徴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。



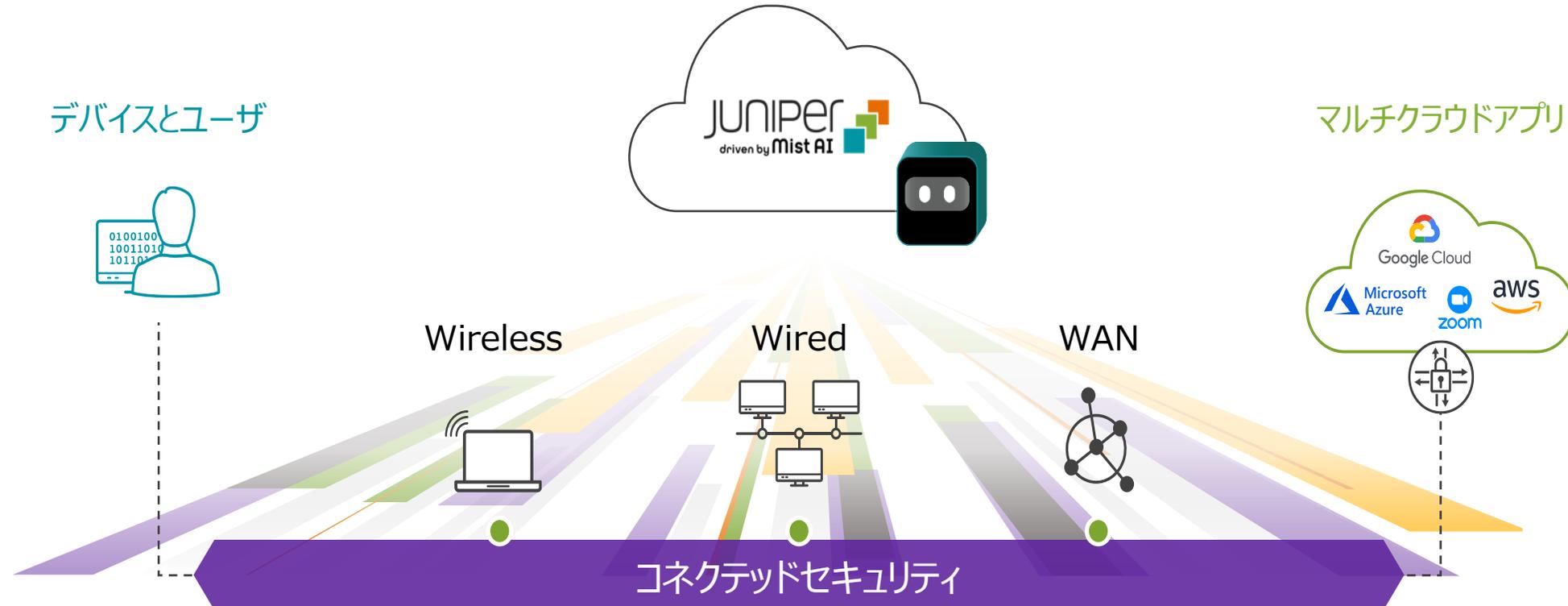
# AI ドリブン SD-WAN

# 業界唯一のエクスペリエンスファースト AI ドリブンフルスタック

最適化された  
確実な体験

AI ドリブンでプロアクティブな  
オペレーション&サポート

オープンでプログラマブルな  
クラウド



# MIST AI ドリブンポートフォリオ



AI ドリブンクラウドサービス

仮想ネットワーク  
アシスタント

## Marvis

- AI ドリブンによる問題解決
- 会話アシスタント



Marvis VNA

## Marvis Actions

- プロアクティブなネットワーク分析と修復
- 包括的なネットワークの可視化



Wi-Fi Assurance



User Engagement



Asset Tracking



IoT Assurance



Wired Assurance



WAN Assurance

## ワイヤレスインフラ



Mist エッジ



AP12



AP32



AP33



AP34



AP43



AP45



AP63  
(屋外)



BT11  
(BLE)

## 有線インフラ



EX4600/4650



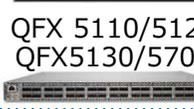
EX4400



EX3400



EX4300



QFX 5110/5120  
QFX5130/5700



EX2300

## WAN インフラ



SRX



セッションスマート  
ルーター

# セッションスマートルーティング

## AI ドリブン SD-WAN

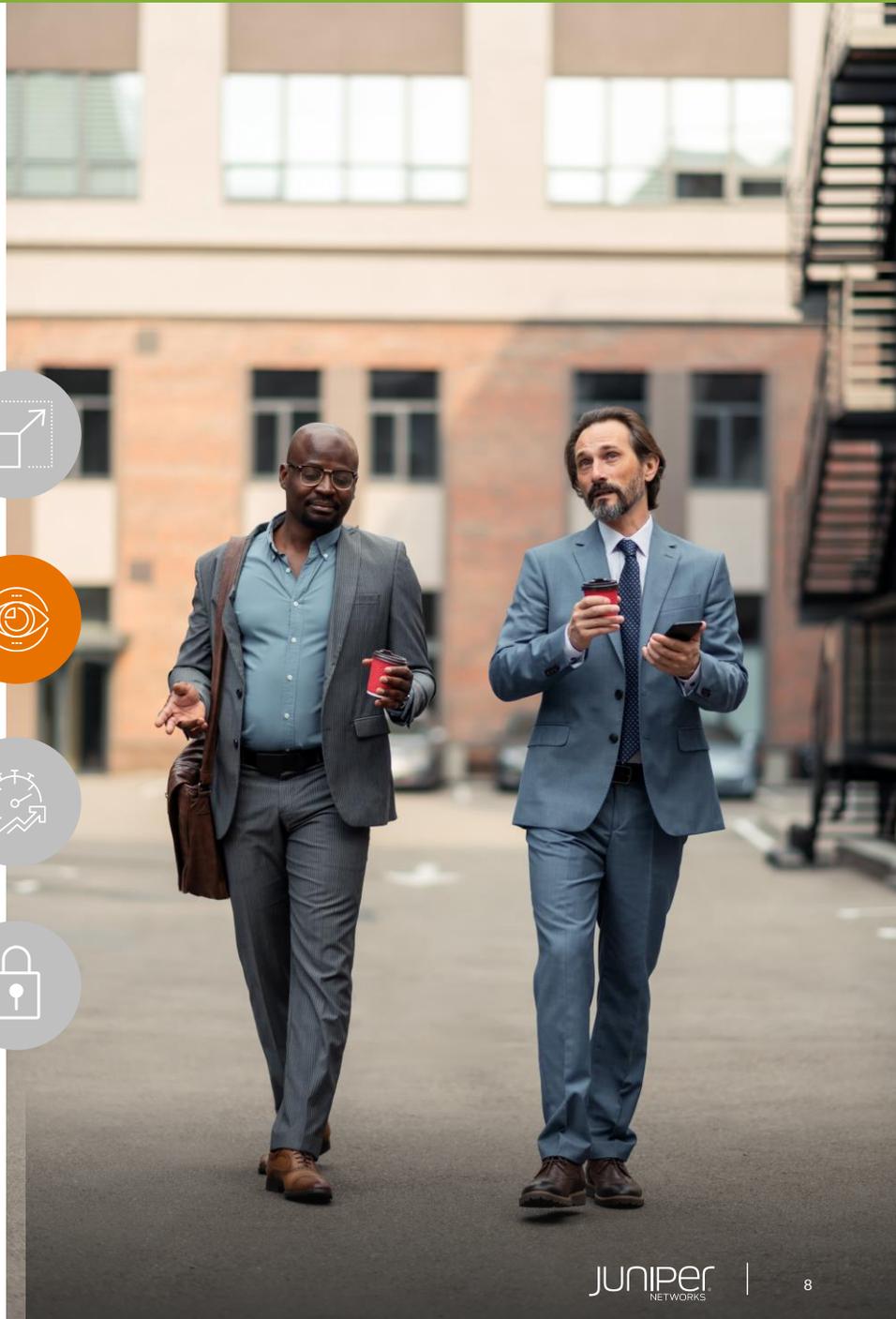
- ✓ アプリケーション基準制御により、セッションポリシーとネットワークステータスに基づいた、重要アプリケーションの優先的な処理とアップタイムを保証
- ✓ グローバルポリシーの集中型オーケストレーションとマイクロサービス型のクラウドアーキテクチャによる、サービス展開の加速化と併せた、数千のサイトへのスケーラビリティ
- ✓ セッションスマートファブリックは、セッション、テナント、および、動的ワークロードのコンテキストをエンドツーエンドで維持し、ネットワークの応答性を向上
- ✓ トンネルレスのアーキテクチャにより、最大 30~50% の帯域幅コストを削減



# WAN Assurance & Marvis VNA

## AI ドリブン SD-WAN

- ✓ **WAN ユーザーエクスペリエンスのリアルタイム可視化**をアプリケーション、リンク、セッションスマートルーター(SSR)、および SRX 機器のヘルス指標の SLE (サービスレベルエクスペリエンス) により実現
- ✓ **Day1 オペレーションの簡素化**を直感的な QR claim code スキャンと、セッションスマートルーター用の設定テンプレートで可能に
- ✓ ゲートウェイの設定ミスや、故障したインターフェイスを **自動的に特定**
- ✓ Marvis Actions による **Self-Driving Network™** フレームワークは、Mist AI を活用し、IT ドメインまたいだ問題の根本原因を特定し、自動修正または推奨アクションを提供



# ユーザーエクスペリエンス

## AI ドライブン SD-WAN

- ✓ VPN 基準のソリューションのように高価なホットスタンバイトンネルを必要とせず、**信頼性の高い高性能な接続**を実現
- ✓ **高粒度な QoS** により、効率的なトラフィックシェーピングと優先順位付け、および、データフロー毎の SLA を適用
- ✓ **サブセカンドフェイルオーバー**は、セッションの最適化とインテリジェントルーティングに対応した多くの機能の一つ
- ✓ **WAN 帯域幅の利用率を高め**、低容量の WAN 接続でのパフォーマンスを向上させながら、ロスの無いアプリケーション配信を可能に



# ゼロトラストネットワークキング

## AI ドリブン SD-WAN

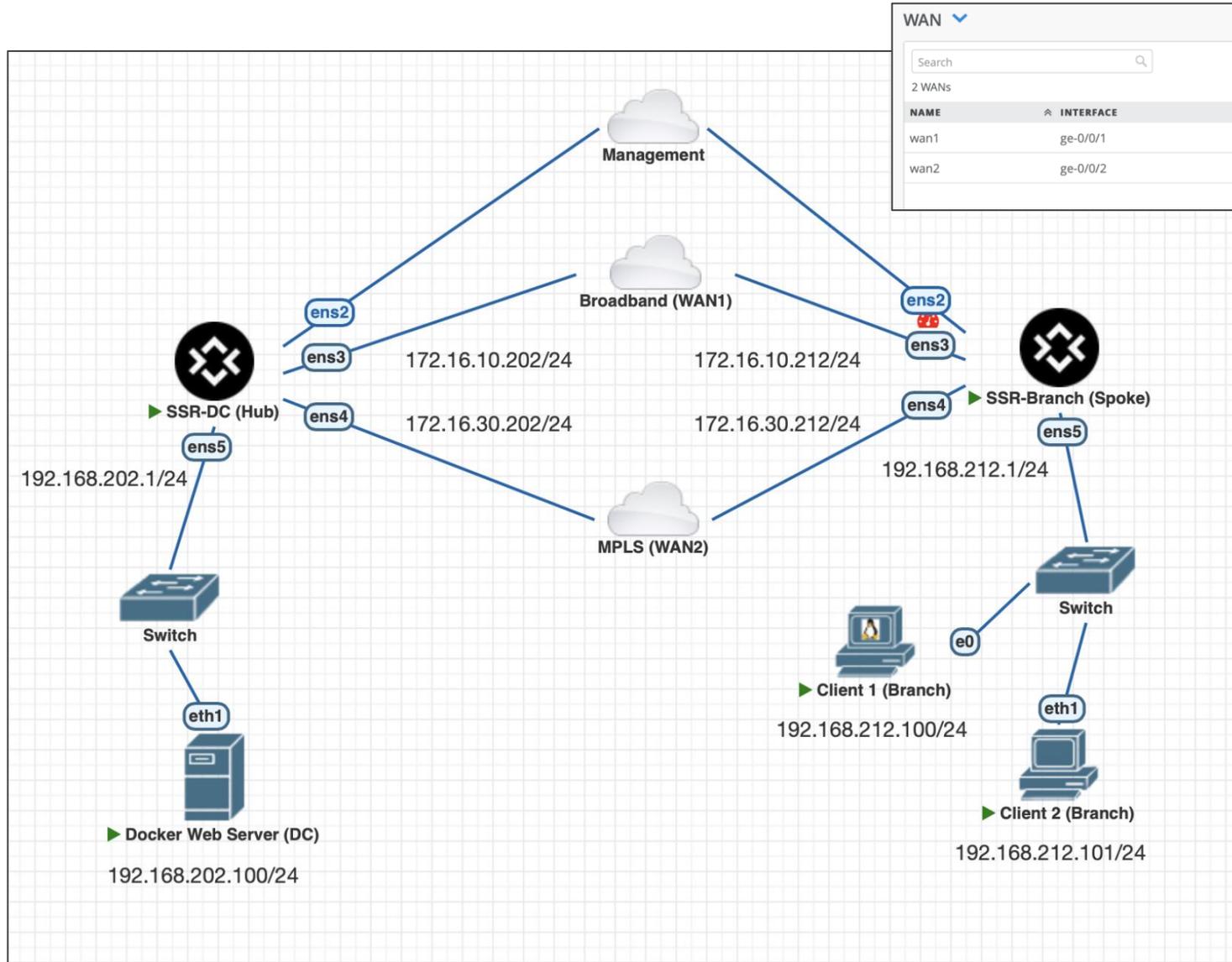
- ✓ デフォルト拒否・マルチホップ認証を特徴とするゼロトラストセキュリティ方式を SD-WAN ファブリックと融合
- ✓ 個々のトラフィックフローを完全に可視化し、エンドツーエンドセッションの効率的な監視、サービス品質の評価、トンネルフリーアーキテクチャによる問題のトラブルシューティングを実現
- ✓ 指向性とセグメンテーションのポリシーを、セキュアベクタールーティング、ゼロトラストのアクセス制御を統合した、セッション認知のファブリックによって執行
- ✓ ネットワークセキュリティパフォーマンスの最適化をセキュアベクタールーティング (SVR) によって可能としながら、不必要な重複暗号やオーバーヘッドによる、ユーザーエクスペリエンスの低下を防止





# デモリファレンス

# デモリファレンスアーキテクチャ



WAN

Search

2 WANs

NAME	INTERFACE	WAN TYPE	IP CONFIGURATION	OVERLAY HUB ENDPOINTS
wan1	ge-0/0/1	Ethernet	172.16.10.212/24	dc1-wan1
wan2	ge-0/0/2	Ethernet	172.16.30.212/24	dc1-wan2

## Spoke でオーバーレイ接続



Edit WAN Configuration

Name

wan1

Overlay Hub Endpoint

dc1-wan1

Edit WAN Configuration

Name

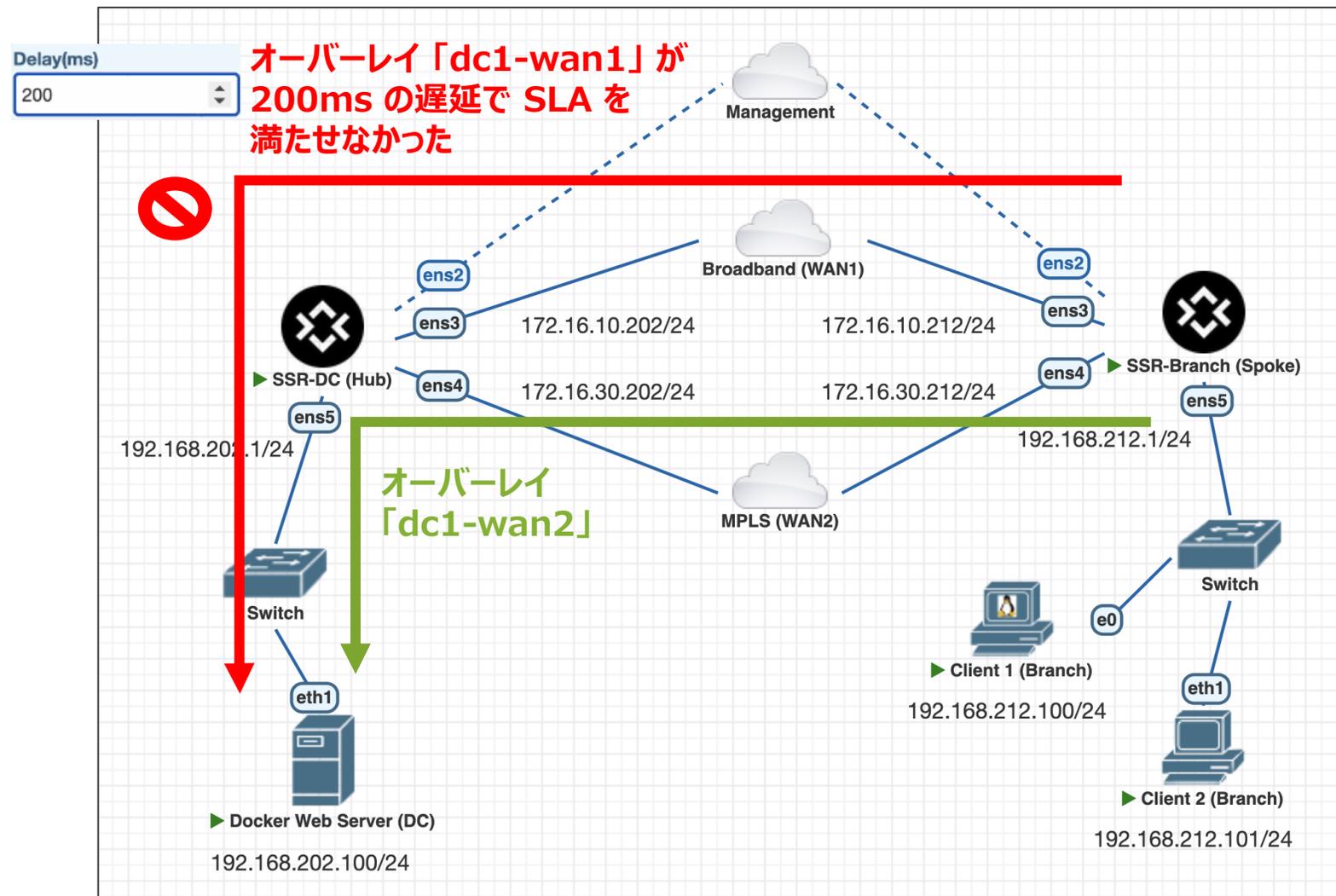
wan2

Overlay Hub Endpoint

dc1-wan2

## ハブの WAN インターフェース

# シナリオ 1 – 動的パス制御



事前定義 SLA を基準とした動的なパス制御

Failover Policy

Revertible  Non-Revertible

Traffic Class

Best Effort

DSCP Class

Maximum Latency

20

Maximum Jitter

10

Maximum Loss

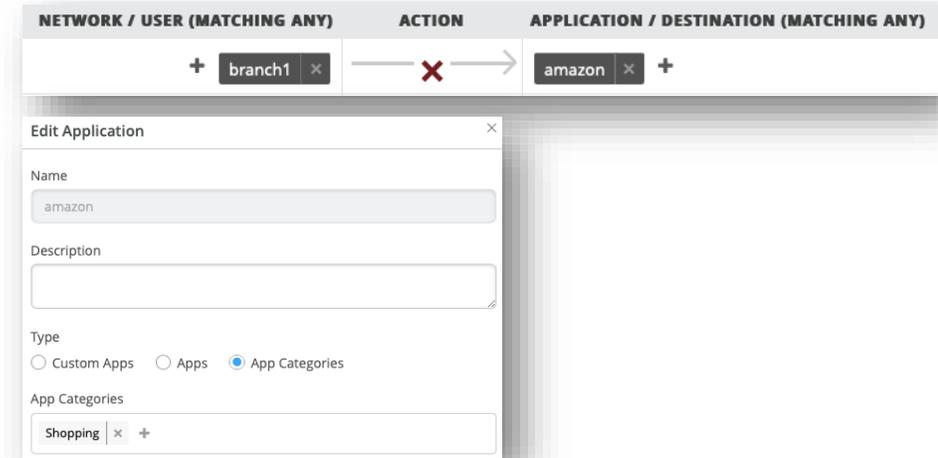
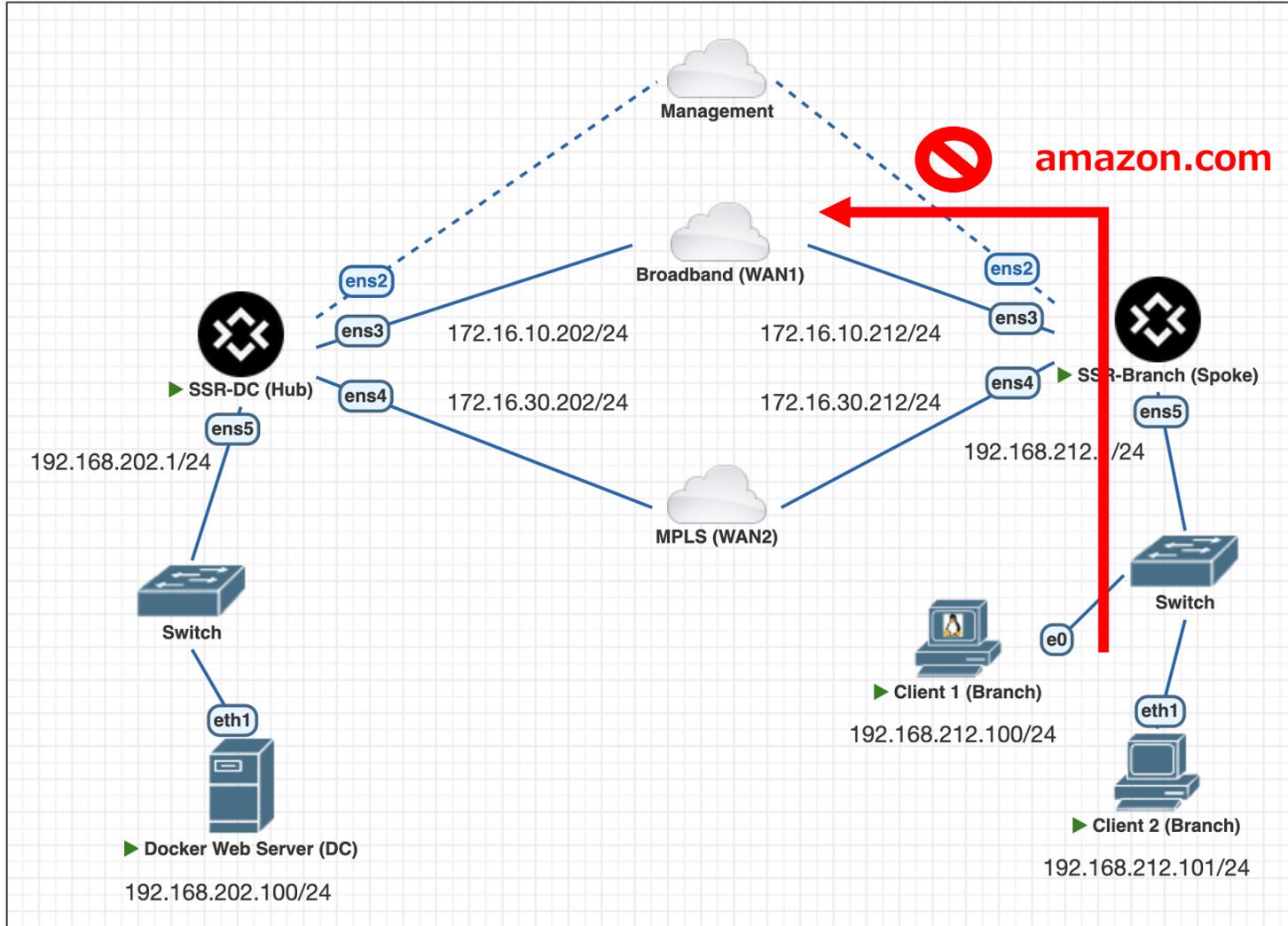
5

高速フェイルオーバー

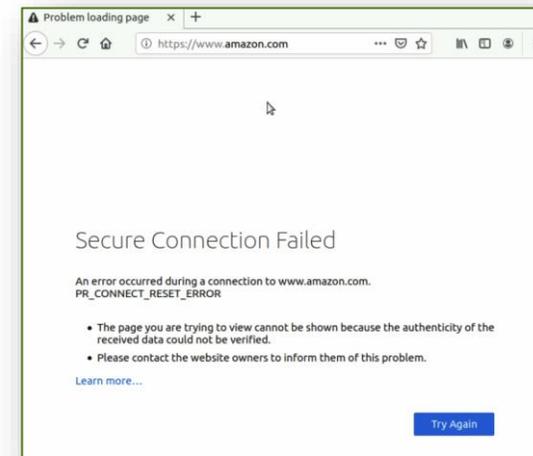
```
64 bytes from 192.168.202.101: icmp_seq=14 ttl=62 time=0.810 ms
64 bytes from 192.168.202.101: icmp_seq=15 ttl=62 time=0.927 ms
64 bytes from 192.168.202.101: icmp_seq=16 ttl=62 time=0.804 ms
64 bytes from 192.168.202.101: icmp_seq=17 ttl=62 time=0.917 ms
64 bytes from 192.168.202.101: icmp_seq=18 ttl=62 time=0.899 ms
64 bytes from 192.168.202.101: icmp_seq=19 ttl=62 time=0.878 ms
64 bytes from 192.168.202.101: icmp_seq=20 ttl=62 time=0.895 ms
64 bytes from 192.168.202.101: icmp_seq=21 ttl=62 time=0.862 ms
64 bytes from 192.168.202.101: icmp_seq=22 ttl=62 time=0.788 ms
64 bytes from 192.168.202.101: icmp_seq=23 ttl=62 time=0.863 ms
64 bytes from 192.168.202.101: icmp_seq=24 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=25 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=26 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=27 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=28 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=29 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=30 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=31 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=32 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=33 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=34 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=35 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=36 ttl=62 time=201 ms
64 bytes from 192.168.202.101: icmp_seq=37 ttl=62 time=6.63 ms
64 bytes from 192.168.202.101: icmp_seq=38 ttl=62 time=0.783 ms
64 bytes from 192.168.202.101: icmp_seq=39 ttl=62 time=0.933 ms
64 bytes from 192.168.202.101: icmp_seq=40 ttl=62 time=0.780 ms
64 bytes from 192.168.202.101: icmp_seq=41 ttl=62 time=0.790 ms
64 bytes from 192.168.202.101: icmp_seq=42 ttl=62 time=0.760 ms
64 bytes from 192.168.202.101: icmp_seq=43 ttl=62 time=0.813 ms
```

# シナリオ 2 – URL フィルタリング

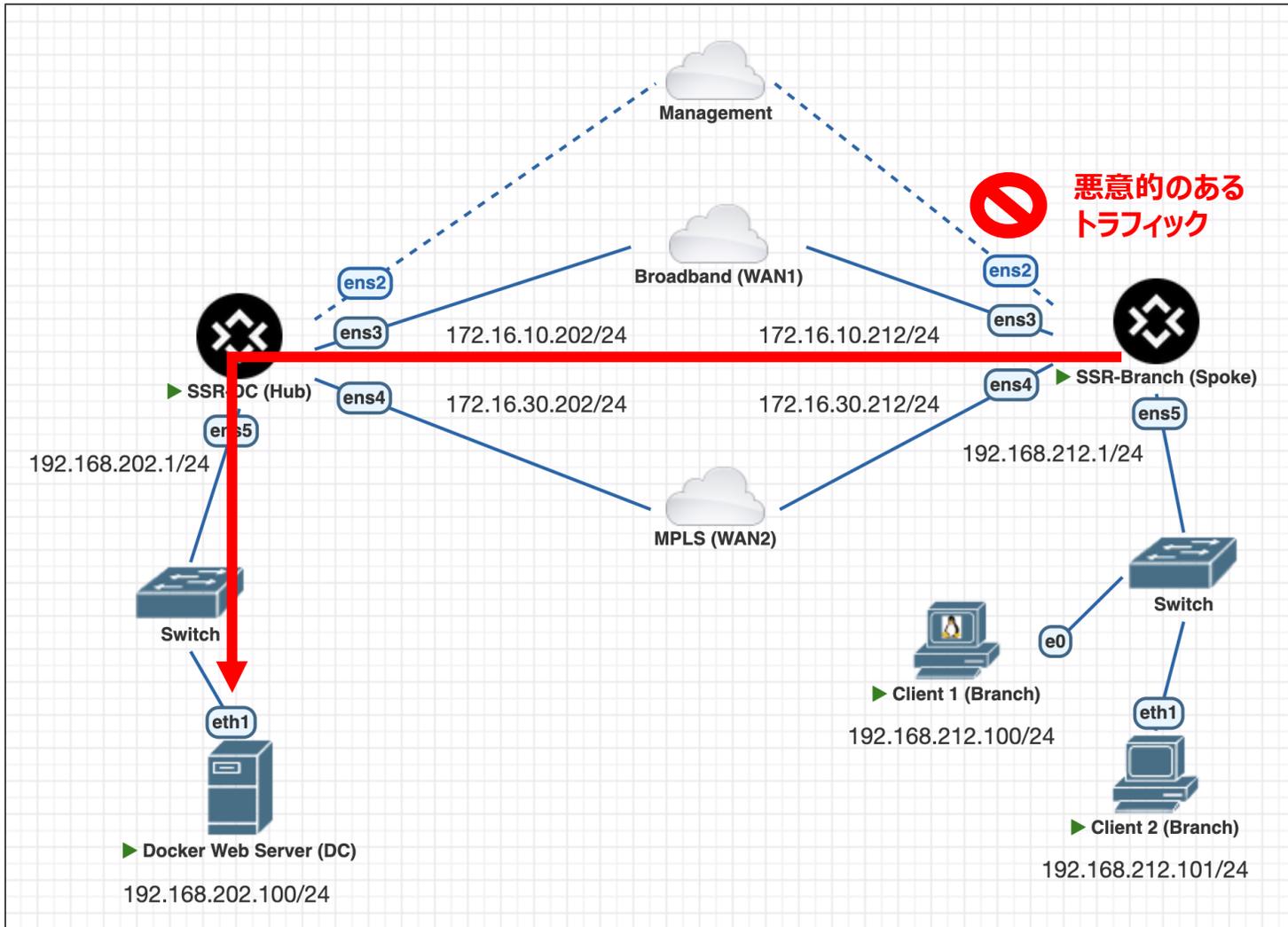
URL フィルタリングによって「amazon.com」へのトラフィックを制限する



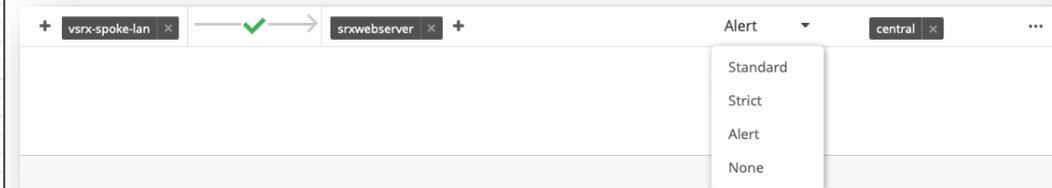
ウェブサイトへのアクセス不可



# シナリオ 3 - IDP



ユーザーから Web サーバーへの悪意のある  
トラフィックを検出・防止する IDP を有効化



## イベント詳細

Secure WAN Edge IDP/URL Events

945 Total

Time	Device Name	Site	Source Address	Source Port	Source Interface	Destination Address	Destination Port	Destination Interface	Attack Name	Threat Severity	Action
2/23/2023, 11:53:29 AM	SSR-Spoke1-Branch1	branch1	192.168.212.101	54110	ge-0-3	192.168.202.101	80	ge-0-2	HTTP:ISSXAIR-DOS	Major	none
2/23/2023, 11:53:29 AM	SSR-Spoke1-Branch1	branch1	192.168.212.101	54110	ge-0-3	192.168.202.101	80	ge-0-2	HTTP:ISSXHTML-SCRIPT-IN-URL-VAR	Major	none
2/23/2023, 11:53:29 AM	SSR-Spoke1-Branch1	branch1	192.168.212.101	54110	ge-0-3	192.168.202.101	80	ge-0-2	HTTP:ISSAMPLE-ACCESS	Minor	none
2/23/2023, 11:53:29 AM	SSR-Spoke1-Branch1	branch1	192.168.212.101	54110	ge-0-3	192.168.202.101	80	ge-0-2	HTTP:ISSQLIN-GENERIC	Minor	none
2/23/2023, 11:53:29 AM	SSR-Spoke1-Branch1	branch1	192.168.212.101	54108	ge-0-3	192.168.202.101	80	ge-0-2	HTTP:ISSXHTML-SCRIPT-IN-URL-VAR	Major	none
2/23/2023, 11:53:29 AM	SSR-Spoke1-Branch1	branch1	192.168.212.101	54110	ge-0-3	192.168.202.101	80	ge-0-2	HTTP:ISSQLIN-REQ-VARS	Minor	none

### Signature Detail

#### HTTP: Generic SQL Injection Detection

This signature detects specific characters, typically used in SQL, within an HTTP connection. Because these characters are not normally used in HTTP, this can indicate a SQL or command injection attack. However, it can be a false positive. To reduce False Positives, it is strongly recommended that these signatures only be used to inspect traffic from the Internet to your organization's web servers that use SQL backend databases to generate content and not to inspect traffic going from your organization to the Internet. Some attempts at Cross Site Scripting attacks also trigger this signature.



# ジュニパーの SASE

# ジュニパーの SASE

## AI ドリブン SD-WAN + Juniper Secure Edge



-  フルスタックブランチオペレーション
-  高度な AI・ML
-  セッションスマートネットワーク
-  ゼロトラスト
-  セグメンテーション

FWaaS

 アプリケーション制御

SWG

 ID とアクセス制御

CASB

 侵入防止

DLP

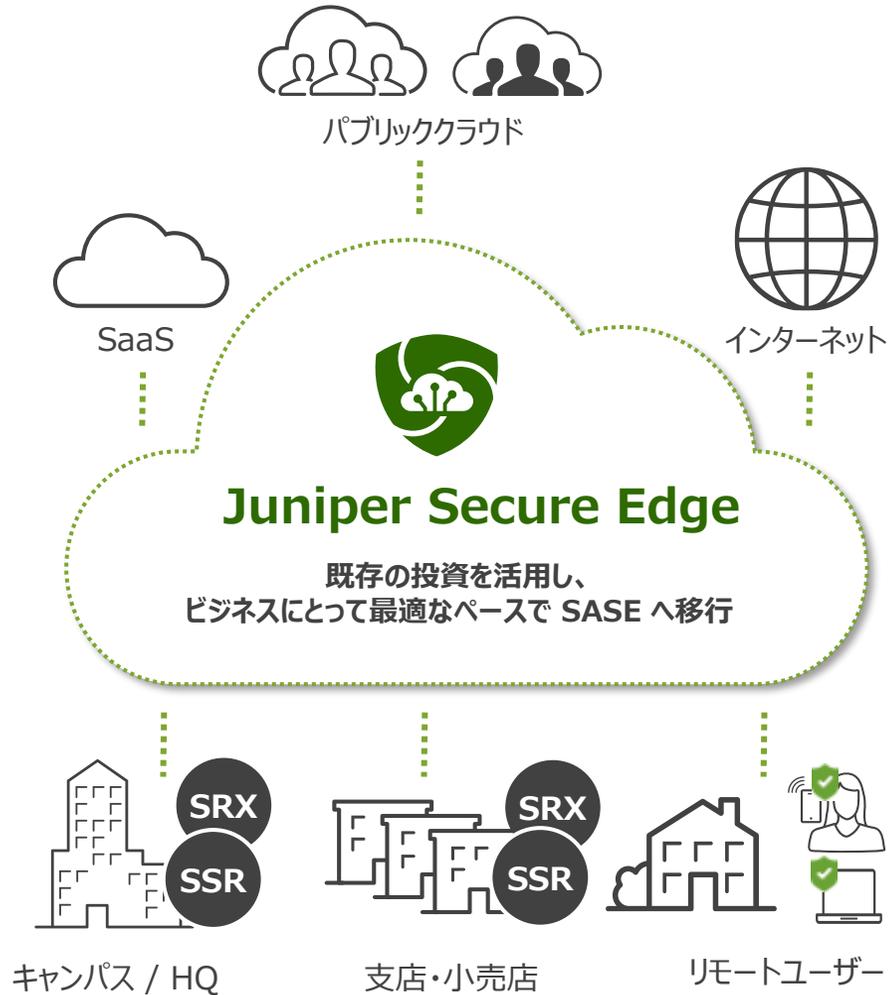
 アンチマルウェア

ZNA

 脅威インテリジェンス

 セキュアウェブアクセス

# ジュニパーの SASE/SSE の魅力



## SASE フルサポート

- SD-WAN + SSE のユースケースをサポート
- どこからでもセキュアなユーザーアクセス
- オンプレミスおよびクラウド上のアプリケーションへのアクセスを保護

## 統一されたセキュリティと有効性

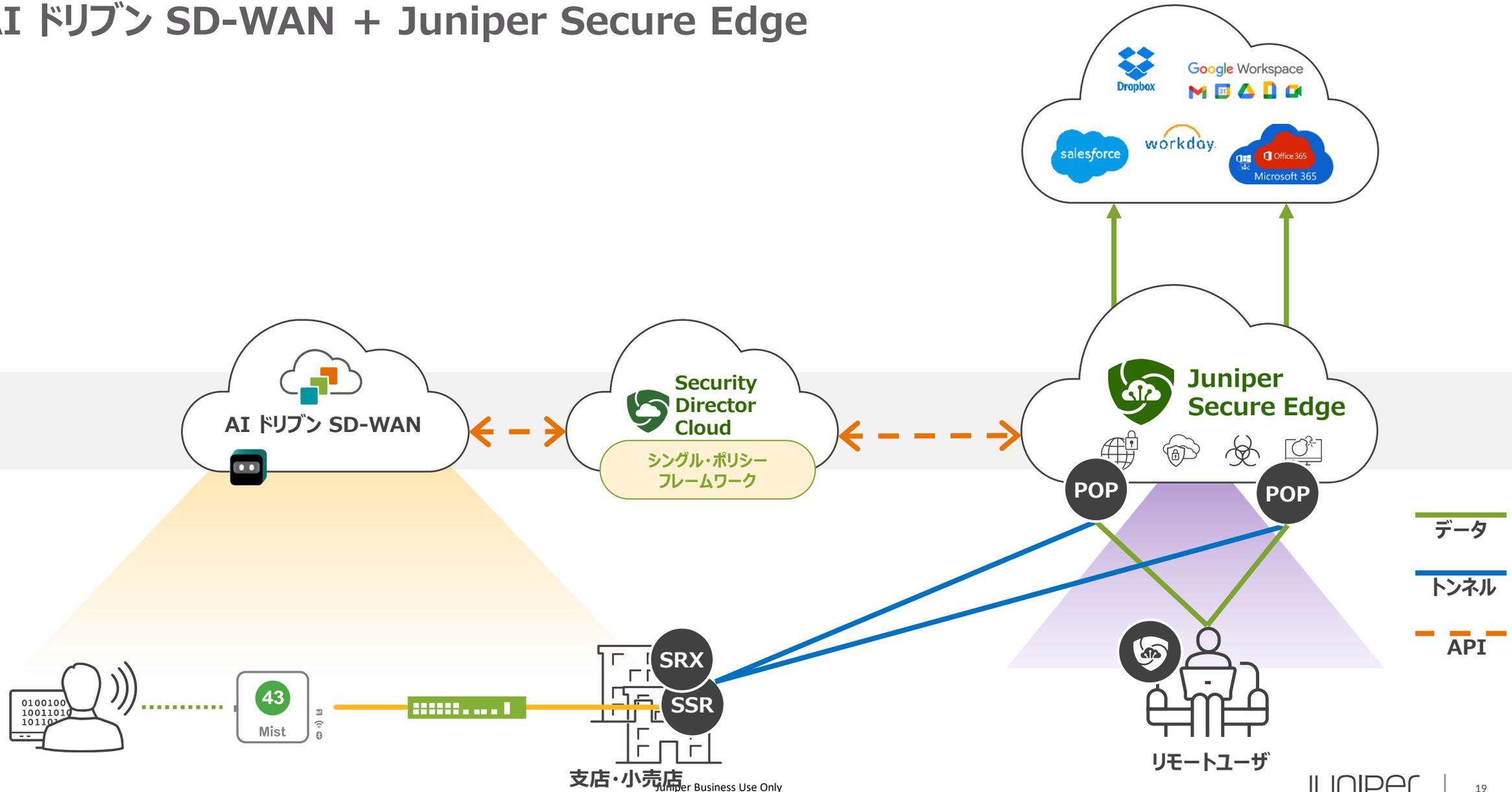
- SD-WAN + SSE をシングルベンダー提供
- お客様単位の専用セキュリティクラウド
- セキュリティの有効性

## フレキシブルなトランジションパス

- 顧客ビジネスに最適なペースでの移行
- 柔軟なライセンスとデプロイメント
- 成長に合わせた支払い

# ジュニパーの SASE が活躍

## AI ドリブン SD-WAN + Juniper Secure Edge



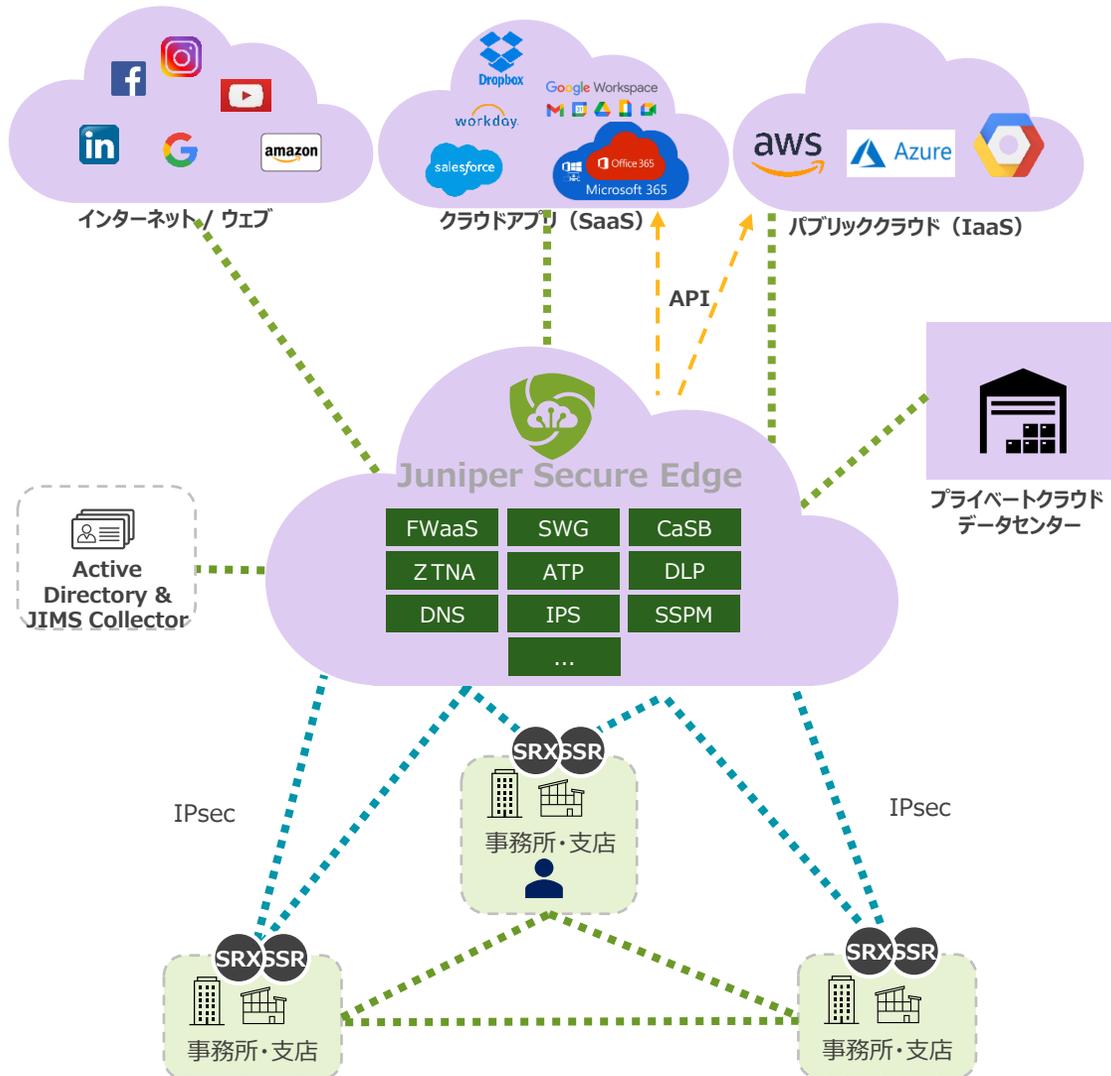
# Juniper Secure Edge

## グローバル 提供拠点 (POP)



# Juniper Secure Edge - ブランチの使用例

## クラウドで実現するセキュリティ - インラインとアウトオブバンド



### 可視化

- すべてのインターネットトラフィック
- すべてのアプリ - 認可・未認可アプリ
- すべてのユーザ - 認証・未認証のユーザ
- すべてのデバイス - 管理・非管理デバイス



### アクセス コントロール

- FWaaS - 統一ポリシー
- JIMS/AD を統合した UserFW
- アドバンスドサービス
- マルウェア対策、IDP、Web フィルタリング、コンテンツフィルタリング、復号化



### 脅威防止

- ATP Cloud と完全統合
- 脅威フィード
- DNS セキュリティ、サンドボックス、暗号トラフィックインサイト



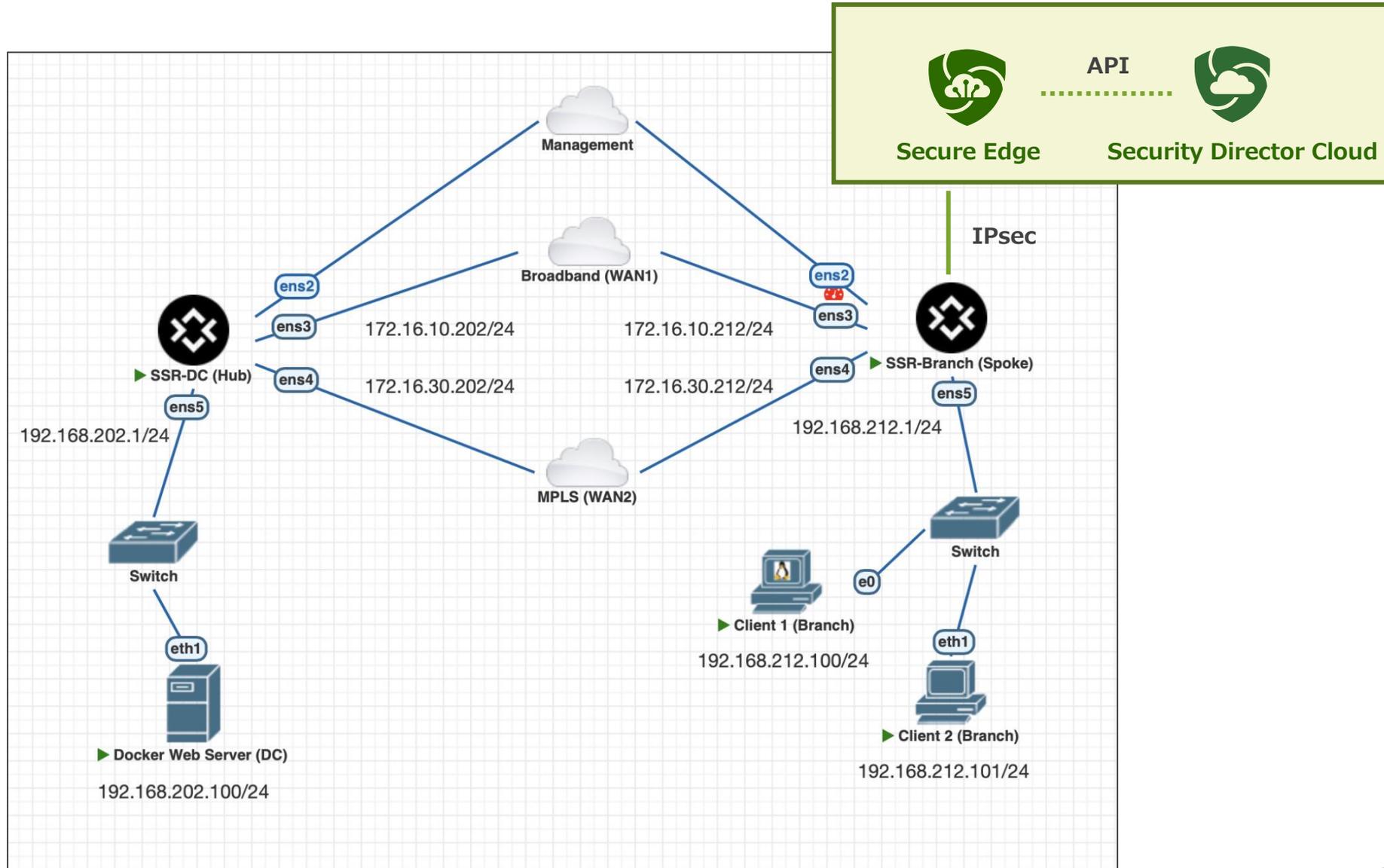
### データ保護

- 動的・静的データ
- CASB
- データ漏洩防止(DLP)
- クラウドデータディスカバリー



# MIST SECURE EDGE の統合

# デモリファレンスアーキテクチャ (Juniper Secure Edge 利用時)





IPsec プロファイル



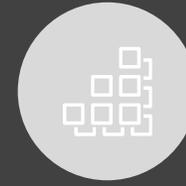
サイト



JSE コネクター



SD-WAN ポリシー



JSE ポリシー



**Create IPsec Profile** ?

Name \* ? aide\_tsc\_lab\_ssr ✓

Description ?

**IKE Settings** IPsec Settings

IKE Auth Method ? PSK ✓

Diffie-Hellman group ? GROUP\_14 ✓

Encryption algorithm ? AES\_128\_GCM ✓

Lifetime seconds ? 86400 ✓

Cancel OK



**Create IPsec Profile** ?

Name \* ? aide\_tsc\_lab\_ssr ✓

Description ?

IKE Settings **IPsec Settings**

Encryption algorithm ? AES\_128\_GCM ✓

Lifetime seconds ? 3600 ✓

Perfect forward secrecy gr... ? GROUP\_14 ✓

Cancel OK

## IPsec 暗号化アルゴリズムプロファイルを設定



IPsec プロファイル



サイト



JSE コネクター



SD-WAN ポリシー



JSE ポリシー

**Create Site** Prerequisite: Two active Service Locations

**Service Locations**

Primary service location \*  ✓

Secondary service location \*  ✓

Number of Users \*

Estimated provisioned bandwidth: 2 Mbps

**Site Details**

Name \*  ✓

Description

Country \*

Postal code

Site address

Protected networks \*  +

Protected Networks	
<input type="checkbox"/>	192.168.212.0/24
<input checked="" type="checkbox"/>	192.168.202.0/24

2 items

**Create Site** Prerequisite: Two active Service Locations

Progress: Site Details | **Traffic Forwarding** | Site Configuration | Summary

**Traffic Forwarding**

Tunnel type  IPsec  GRE

IP address type  Dynamic  Static

IPsec profile \*  [Create IPsec Profile](#)

Pre-shared key \*

IKE ID \*

**Create Site** Prerequisite: Two active Service Locations

Progress: Site Details | Traffic Forwarding | **Site Configuration** | Summary

**Site Configuration**

Devices Type \*  Juniper Device  Non-Juniper Device

No configuration input required for Non-Juniper device. You may proceed to the next step.

**Service Locations**

Primary service location jsec-tokyo

Secondary service location jsec-singapore

Number of Users 5

Estimated provisioned bandwidth: 2 Mbps

**Site Details**

Name csodemo2

Description --

Country Hong Kong

Postal code --

Site address --

Protected networks 192.168.212.0/24,192.168.202.0/24

**Traffic Forwarding**

Tunnel type IPsec

IP address type Dynamic

IPsec profile aide\_tsc\_lab\_ssr

Pre-shared key \*\*\*\*\*

IKE ID alexchan@juniper.net

## POP 接続用のサイトを作成





IPsec プロファイル



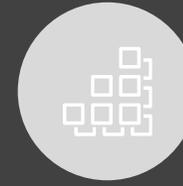
サイト



JSE コネクター



SD-WAN ポリシー



JSE ポリシー

TRAFFIC STEERING

Search

2 Traffic Steering

Add Traffic Steering

# JSE パスでトラフィックの制御プロファイルを作成

APPLICATION POLICIES

Search

Displaying 1 of 1 total Application Policy

Import Application Policy

Add Application Policy

Edit Applications

NO.	NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	TRAFFIC STEERING
1	Policy-1	+ branch1	→ ✓	internet +	None	JSE

Add Traffic Steering

Name

JSE

Strategy

Ordered

Weighted

ECMP

PATHS

Add Paths

Add Path

Type

Secure Edge Connector

Provider

Juniper Secure Edge (IPsec Only)

Name

JSE

# トラフィック制御をアプリケーションポリシーに付加する



IPsec プロファイル



サイト



JSE コネクター



SD-WAN ポリシー



JSE ポリシー

## デフォルトで拒否のため、セキュリティポリシーを追加してトラフィックを許可

<input checked="" type="checkbox"/>	2	csodemo2	csodemo2	Any	Any	Any	Permit	IPS Decrypt Web Filtering
	17.1K hits	Any						Content Filtering Secintel
								Anti-malware

## セキュリティ保護機能を有効化

IPS profile

Decrypt profile  [Create New](#)

Web filtering  [Create New](#)

Content filtering  [Create New](#)

Secintel group  [Create New](#)

Anti-malware

admin / Juniper123123



# サマリー

# サマリー

1. Mist が提供する「フルスタック」で包括的な AI ドリブン SD-WAN
2. パートナー向けデモリファレンス材料の提供
3. JSE との統合によるセキュリティ機能強化



# リソース

# リソース

## 公開動画：

- [セッションスマートルーター ブランチセキュリティパックの概要](#)
- [マイクと Marvis が WAN Assurance を解説](#)
- [AI ドリブン SD-WAN のヒーロー紹介](#) (新しいしいデモや動画を掲載中！)

## ウェビナー&イベント

- オンデマンド配信：[Mist AI ドリブンのジュニパー SD-WAN デモ](#)
- オンデマンド配信：[政府機関にセキュアな SD-WAN を供給](#)



# THANK YOU

JUNIPER  
NETWORKS

Driven by  
Experience™