ポリシーグループを使用したセキュリティポリシー

ポリシーグループを使用したセキュリティポリシー

ポリシーグループを使用したセキュリティポリシー

表 *1*: 機能の履歴

機能名	リリース情報	説明
ポリシーグループを使用したセキュリティポリシー		この機能は、セキュリティポリシーの設定にシンプルで再利用可能な構造化されたアプローチを提供します。ネットワーク内の1つ以上のサイト、またはサイトの単一のデバイスに適用されるポリシーの論理グループ（セキュリティポリシー）を作成できます。 ポリシーグループ展開ワークフローでは、以前に作成したポリシーグループを選択し、設定グループによって管理されているサイトまたはサイトの単一のデバイスにそれらを展開するための、ガイド付きの手法が提供されます。

セキュリティポリシーに関する情報

ポリシーグループを使用してセキュリティポリシーを設定すると、SD ルーティングデバイスでのポリシーの設定および展開操作が簡素化されます。ワークフローを使用してポリシーを設定し、それらのポリシーをネットワーク内のデバイスに関連付けます。

[Policy Groups] ページには、次のものが含まれます。

- **ポリシー グループ**
- **組み込みセキュリティ設定**
- **DNS セキュリティ設定**

セキュリティポリシーの RBAC の有効化

設定グループを使用してポリシーグループおよびセキュリティ機能プロファイルを作成するには、ロールベースアクセスコントロール（RBAC）で、各機能にアクセスするための読み取りおよび書き込み権限を次のプロファイルに付与する必要があります。**[Configuration]** > **[Policy Groups]**から、ポリシーグループにアクセスできるようにユーザーグループの権限を設定してください。

1. Cisco Catalyst SD-WAN Manager のメニューから、**[Administration]** > **[Manage Users]** > **[User Groups]**の順に選択します。
2. [Add a User Group] をクリックします。

3. [User Group Name] を入力します。
4. ユーザーグループに割り当てるポリシーグループ機能（[Policy Group]）、デバイス機能（[Device]）、および展開機能（[Deploy]）に関して、[Read] または [Write] チェックボックスをオンにします。
5. ユーザーグループに割り当てる次の機能に関して、[Read] または [Write] チェックボックスをオンにします。
   - **[Feature Profile]** > **[Embedded Security]** > **[Legacy Policy]**
   - **[Feature Profile]** > **[Embedded Security]** > **[NGFirewall]**
   - **[Feature Profile]** > **[Embedded Security]** > **[Policy]**
   - **[Feature Profile]** > **[Policy Object]** > **[Advanced Inspection Profile]**

     [Advanced Inspection Profile] には、次のサブ機能プロファイルがあります。
     - 高度なマルウェア防御
     - 侵入防御
     - SSL 復号
     - SSL 復号プロファイル
     - URL フィルタリング
6. [Add] をクリックします。

セキュリティポリシーに関する制約事項

セキュリティポリシーは、カスタム定義のアプリケーションリストに含まれるカスタムアプリケーションを使用したトラフィックの照合をサポートしていません。

ポリシーグループを使用したセキュリティポリシーの設定

セキュリティポリシー作成ワークフローを使用して、セキュリティポリシーの作成、サブポリシーの追加、既存のサブポリシーへのルールの追加などを行うことができます。

1. Cisco SD-WAN Manager のメニューから、**[Workflows]** > **[Workflow Library]** > **[Create Security Policy]**の順に選択します。または、**[Configuration]** > **[Policy Groups]**の順に選択します。
2. [Embedded Security] をクリックします。

3. [Embedded Security] ページで、[Add Security Policy] をクリックします。セキュリティ ポリシー ワークフローが起動します。
4. [Policy Name] にポリシー名を入力し、[Description] に説明を入力して、[Next] をクリックします。
5. [Select the optional Configuration Group to associate with the security policy] ページで、設定グループを選択し、[Next] をクリックします。
6. [Add Sub-Policy] をクリックします。
7. [Submit] をクリックします。[Embedded Security] タブで新しいセキュリティポリシーを表示できます。

セキュリティポリシーの対象グループの設定

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policy Groups]** > **[Group of Interest]**の順に選択します。
2. [セキュリティ（Security）] タブをクリックします。セキュリティオブジェクトとプロファイルのリストが表示されます。

セキュリティポリシーに別のリストグループを設定するには、次の表を使用します。

アプリケーション

フィールド	説明
[Application List Name]	アプリケーションリストの名前。
[Applications]	ドロップダウンリストから 1 つ以上のアプリケーションタイプを選択します。たとえば、サードパーティコントロール、ABC News、Microsoft Teams などです。 ドロップダウンリストから 1 つ以上のアプリケーション ファミリ タイプを選択します。たとえば、[application-service]、[audio_video]、[authentication]、[behavioral]、[compression]、[database]、[encrypted] などです。

データプレフィックス

フィールド	説明
[Data Prefix List Name]	プレフィックスリストの名前。
[Data Prefix]	データプレフィックス値。

ローカルドメイン

フィールド	説明
[Local Domain List Name]	ローカルドメインリストの名前。
[Local Domain]	カンマで区切られたローカルドメイン値。たとえば、cisco.com です。

FQDN（完全修飾ドメイン名）

FQDNは、データセンターまたはプライベートクラウド内のスタンドアロンサーバーの照合に使用することを目的としています。パブリックURLを照合する場合、推奨される照合アクションは**ドロップ**です。パブリックURLに対して**inspect**を使用する場合は、関連するすべてのサブURLおよびリダイレクトURLを定義する必要があります。

フィールド	説明
[FQDN List Name]	FQDN リストの名前。
FQDN	カンマで区切られたURL名。たとえば、cisco.com です。

署名

署名セットは、共通脆弱性評価システム（CVSS）スコアが9以上の脆弱性をブロックします。また、過去2年間に公開され、マルウェアCNC、エクスプロイトキット、SQLインジェクション、またはブロックリストのルールカテゴリを持つCVE（Common Vulnerabilities and Exposures）もブロックします。

フィールド	説明
[IPS Signature List Name]	IPS 署名リストの名前。
[IPS Signature]	カンマで区切られた「ジェネレータ ID:署名 ID」形式の署名。たとえば、1234:5678 です。 範囲は 0 ～ 4294967295 です。

URL 許可

リストベースのフィルタリングにより、ユーザーは、許可リストまたはブロックリストに基づくアクセス許可またはアクセス拒否を行いアクセスを制御できます。これらのリストに関して注意が必要な重要項目は、次のとおりです。

- 許可されたURLは、カテゴリベースのフィルタリングの対象になりません。
- 許可リストとブロックリストの両方で同じ項目が設定されている場合、トラフィックは許可されます。

- トラフィックが許可リストとブロックリストのどちらにも一致しない場合、そのトラフィックはカテゴリベースおよびレピュテーションベースのフィルタリングの対象となります。

フィールド	説明
[Allow URL List Name]	許可URLリストの名前。
[Allow URL]	許可する URL。

URL ブロック

リストベースのフィルタリングにより、ユーザーは、許可リストまたはブロックリストに基づくアクセス許可またはアクセス拒否を行いアクセスを制御できます。

フィールド	説明
[Block URL List Name]	ブロック URL リストの名前。
[Block URL]	ブロックする URL。

ゾーン

フィールド	説明
[Zone List Name]	ゾーンリストの名前。
VPN	ゾーンタイプが「**VPN**」のゾーンを設定することを選択します。ドロップダウンリストから VPN をゾーンに追加します。次のオプションがあります。 • [Payment Processing Network] • [Corporate Users] • [Local Internet for Guests] • [Physical Security Devices]

フィールド	説明
Interface	ゾーンタイプが「**インターフェイス**」のゾーンを設定することを選択します。[Add Interface] ドロップダウンリストからインターフェイスをゾーンに追加します。次のオプションがあります。 • Ethernet • FastEthernet • FiveGigabitEthernet • FortyGigabitEthernet • GigabitEthernet • HundredGigE

ポート

フィールド	説明
[Port List Name]	ポートリストの名前。
Port	カンマで区切られたポート値。 範囲は 0 ～ 65530 です

プロトコル

フィールド	説明
[Protocol List Name]	プロトコルリストの名前。
Protocols	ドロップダウンリストから 1 つ以上のプロトコル名を選択します。たとえば、[snmp]、[tcp]、[udp]、[icmp]、[echo]、[telnet] などです。

位置情報

フィールド	説明
[Geo Location List Name]	地理位置情報リストの名前。
[Geo Location]	ドロップダウンリストから 1 つ以上の地理位置情報を選択します。たとえば、[Africa]、[Antartic]、[Asia]、[Europe] などです。

対象のセキュリティグループには、次のプロファイルがあります。

- 詳細な検査プロファイル
- 侵入防御ポリシー
- URL フィルタリング
- 高度なマルウェア防御
- TLS/SSL プロファイル
- TLS/SSL 復号

詳細な検査プロファイル

フィールド	説明
[Profile Name]	詳細な検査プロファイルの名前。
[Description]	プロファイルの説明です。
[Select an Intrusion Prevention]	ドロップダウンリストから侵入防御オプションを選択します。
[Select an URL Filter]	ドロップダウンリストから URL フィルタを選択します。
[Select an Advanced Malware Protection]	高度なマルウェア防御を選択します。
[TLS Action]	TLS アクションを選択します。次のオプションがあります。 • 復号（Decrypt） • パススルー（Pass Through） • [復号しない（Do not Decrypt）]

侵入防御ポリシー

フィールド	説明
[Profile Name]	侵入防御ポリシーの名前。

フィールド	説明
[Signature Set]	[Signature Set] ドロップダウンリストから、トラフィックを評価するためのルールを定義する署名セットを選択します。選択できるオプションは、次のとおりです。 • [Balanced]：システムパフォーマンスに大きな影響を与えることなく保護されます。 • [Connectivity]：制限を緩和し、より少ないルールを課すことでより良いパフォーマンスを提供します。 • [Security]：[Balanced] よりも高い保護を提供しますが、パフォーマンスに影響を与えます。
[Inspection Mode]	検査モードを選択します。次のオプションを使用できます。 • [Detection]：侵入検出モードにはこのオプションを選択します。 • [Protection]：侵入防御モードにはこのオプションを選択します。
[Custom Signature Set]	ドロップダウンリストから 1 つ以上の Web カテゴリを選択します。カテゴリは、[abortion]、[abused-drugs]、[auctions] などです。
[Select an Signature Allow List]	署名許可リストを選択します。
[Alerts Log Level]	アラートログレベルを選択します。 • エラー • 緊急 • アラート • 深刻 • 警告 • 通知 • 情報 • デバッグ

URL フィルタリングポリシー

フィールド	説明
[Profile Name]	URL フィルタリングポリシーの名前。

フィールド	説明
[Web Category]	Web カテゴリを選択します。オプションは、[Block] と [Allow] です。
Web Reputation	ドロップダウンリストから Web レピュテーションを選択します。レピュテーションのオプションは、次のとおりです。 • 高リスク • 不審 • 中リスク • 低リスク • 高信頼性
[Select one or more web categories]	ドロップダウンリストから 1 つ以上の Web カテゴリを選択します。カテゴリは、[abortion]、[abused-drugs]、[auctions] などです。
[Select allow URL list]	許可 URL リストを選択します。
[Select block URL list]	ブロック URL リストを選択します。
[Block Page Server]	次のいずれかのオプションを選択します。 • [Block Page Content]：デフォルトのコンテンツヘッダーとコンテンツ本文を入力します。 • [Redirect URL]：リダイレクト URL を入力します。
[Alerts and Logs]	アラートとログのタイプを選択します。 • ブロックリスト • 許可リスト • レピュテーション/カテゴリ

高度なマルウェア防御ポリシー

フィールド	説明
[Profile Name]	高度なマルウェア防御ポリシーの名前。

フィールド	説明
[Select AMP Cloud Region]	AMT クラウドリージョンを選択します。次のオプションがあります。 • NAM • EU • APJC
[Alert Log Level]	アラートログレベルを選択します。次のオプションがあります。 • 深刻 • 警告 • 情報
[File Analysis]	ファイル分析を有効にします。
[Select TG Cloud Region]	TG クラウドリージョンを選択します。オプションは、[NAM] と [EU] です。
[Select one or more file types]	1 つ以上のファイルタイプを選択します。オプションは、[pdf]、[ms-exe]、[new-office]、[rtf]、[mdb]、[mscab]、[msole2]、[wri]、[xlw]、[flv]、および [swf] です。

TLS/SSL プロファイル

フィールド	説明
[Profile Name]	TLS/SSL プロファイルの名前。
[Select Categories to assign action]	アクション間のカテゴリ（[Decrypt]、[No Decrypt]、および [Pass Through] URL カテゴリ）を設定します。 または、複数のカテゴリを選択してアクションを設定します。
[Reputation]	レピュテーションを有効にして、[Decrypt Threshold] を選択します。復号しきい値のオプションは、次のとおりです。 • 高リスク • 不審 • 中リスク • 低リスク • 高信頼性

フィールド	説明
高度なオプション	
[Select a Decrypt Domain list]	復号ドメインリストを選択するか、[Create New] をクリックして新しい復号ドメインリストを作成します。 **1.** [Decrypt Domain List Name] に復号ドメインリスト名を入力します。 **2.** [Decrypt Domain] に復号ドメインを入力します。 **3.** [Add] をクリックします。
[Select a No Decrypt Domain list]	復号なしドメインリストを選択するか、[Create New] をクリックして新しい復号なしドメインリストを作成します。 **1.** [No Decrypt Domain List Name] に復号なしドメインリスト名を入力します。 **2.** [No Decrypt Domain] に復号なしドメインを入力します。 **3.** [Add] をクリックします。
[Fail Decrypt]	復号に失敗する場合は、[fail decrypt] オプションを有効にします。

TLS/SSL 復号

フィールド名	説明
Policy Name	ポリシーの名前。名前は、最大32文字まで使用できます。
[Server Certificate Checks]	
Expired Certificate	サーバー証明書の有効期限が切れた場合のポリシーの動作を定義します。次のオプションがあります。 • [Drop]：トラフィックをドロップします。 • [Decrypt]：トラフィックを復号します。
[Untrusted Certificate]	サーバー証明書が信頼されていない場合のポリシーの動作を定義します。次のオプションがあります。 • [Drop]：トラフィックをドロップします。 • [Decrypt]：トラフィックを復号します。

フィールド名	説明
[Certificate Revocation Status]	サーバー証明書の失効ステータスをチェックするためにオンライン証明書ステータスプロトコル（OCSP）を使用するかどうかを定義します。オプションは、[Enabled] または [Disabled] です。
[Unknown Revocation Status]	OCSP失効ステータスが不明な場合のポリシーの動作を定義します。 • [Drop]：トラフィックをドロップします。 • [Decrypt]：トラフィックを復号します。
[Unsupported Mode Checks]	
[Unsupported Protocol Versions]	サポートされていないプロトコルのバージョンを定義します。 • [Drop]：サポートされていないプロトコルバージョンをドロップします。 • [Decrypt]：サポートされていないプロトコルバージョンを復号します。
[Unsupported Cipher Suites]	サポートされていない暗号スイートを定義します。 • [Drop]：サポートされていない暗号スイートをドロップします。 • [Decrypt]：サポートされていない暗号スイートを復号します。
[Failure Mode]	障害モードを定義します。オプションは、[close] と [open] です。
[Certificate Bundle]	デフォルトのCAを使用するには、[Use default CA certificate bundle] チェックボックスをオンにします。
[Minimum TLS Version]	プロキシがサポートする必要のある TLS の最小バージョンを設定します。次のオプションがあります。 • **TLS 1.0** • **TLS 1.1** • **TLS 1.2**

フィールド名	説明
[Proxy Certificate Attributes]	
[RSA Keypair Modules]	プロキシ証明書の RSA キー係数を定義します。次のオプションがあります。 • [1024 bit RSA] • [2048 bit RSA] • [4096 bit RSA]
[Ec Key Type]	キータイプを定義します。次のオプションがあります。 • [P256] • [P384] • [P521]
[Certificate Lifetime (in Days)]	プロキシ証明書の有効期間を日数で設定します。

組み込みセキュリティの設定

セキュリティは、今日のネットワーキング インフラストラクチャの非常に重要な要素です。ネットワーク管理者とセキュリティ担当者は、攻撃や侵害からネットワークを防御することを強く求められています。ハイブリッドクラウドとリモート従業員接続のために、ネットワークのセキュリティ境界がなくなりつつあります。

アプリケーション認識機能を備えたエンタープライズ ファイアウォールは、従来のインターフェイスベースのモデルとは異なり、柔軟で理解しやすいゾーンベースのモデルを使用してデータトラフィックを検査します。

ファイアウォールポリシーは、TCP、UDP、および ICMP データトラフィックフローのステートフル検査を可能にするローカライズされたセキュリティポリシーの一種です。特定のゾーンから発信されたトラフィックフローは、2 つのゾーン間のポリシーに基づいて別のゾーンに進むことが許可されます。ゾーンは、1 つ以上の VPN をグループ化したものです。VPN をゾーンにグループ化すると、オーバーレイネットワークにセキュリティ境界を確立できるため、ゾーン間を通過するすべてのデータトラフィックを制御できます。組み込みセキュリティの詳細については、「アプリケーション認識型のエンタープライズファイアウォール」を参照してください。

1. Cisco SD-WAN Manager から、**[Policy Groups]** > **[Embedded Security]**の順に選択します。
2. セキュリティポリシーを選択し、[Edit] をクリックします。
3. [Add Rule] をクリックします。

フィールド	説明
Rule Name	ルールの名前。
Sequence	順序を指定します。
Destination Zone	[Destination Zone] ドロップダウンリストで、データトラフィックの送信先のゾーンを選択します。次のオプションがあります。 • [No-Zone] • [Corporate_Users] • [Local_Internet_for_Guests] • [Payment_Processing_Network] • [Physical_Security_Devices] • [Self] • [Untrusted] ゾーンは、セキュリティポリシー作成ワークフローで選択した設定グループ内のVPNに基づいて作成されます。

フィールド	説明

Match	[Add Conditions] ドロップダウンリストから目的の一致条件を選択します。次のオプションがあります。
	• アプリケーション
	• プロトコル
	• 送信元
	  • 位置情報
	  • IPv4 プレフィックス
	  • ポート
	• 接続先
	  • [FQDN]
	  • 位置情報
	  • IPv4 プレフィックス
	  • ポート
	
	ISE が有効になっている場合、[Source] と [Destination] で SGT オプションを使用できます。アイデンティティユーザーまたはユーザーグループは、[Source] でのみサポートされます。

Action	目的のアクション条件を選択します。次のオプションがあります。 • Pass • Drop • Inspect • [Log Events]：検査アクションの統一されたロギング。ドロップダウンリストから [Advanced Inspection Profile] を選択します。

組み込みセキュリティサブポリシーの設定

1. **[Configuration]** > **[Policy Groups]**から、[Embedded Security] を選択します。
2. リストからセキュリティポリシーを選択し、[Edit] をクリックして、次の詳細を入力します。
3. [Add Sub-Policy] をクリックし、セキュリティポリシーのサブポリシーを追加します。

フィールド	説明
[VPN / Interface]	VPN またはインターフェイスを指定します。
[Source Zone]	データパケットの送信元であるゾーンを選択します。
[Zone List Name]	ゾーンリストの名前。
VPN	ゾーンタイプが「**VPN**」のゾーンを設定することを選択します。ドロップダウンリストからVPNをゾーンに追加します。次のオプションがあります。 • [Payment Processing Network] • [Corporate Users] • [Local Internet for Guests] • [Physical Security Devices]
Interface	ゾーンタイプが「**インターフェイス**」のゾーンを設定することを選択します。[Add Interface] ドロップダウンリストからインターフェイスをゾーンに追加します。
Rule Name	ルールの名前。
Sequence	順序を指定します。

フィールド	説明
Destination Zone	データトラフィックの送信先のゾーンを選択します。次のオプションがあります。 • [Any] • [Corporate_Users] • [Local_Internet_for_Guests] • [Payment_Processing_Network] • [Physical_Security_Devices] • [Self] • [Untrusted (VPN 0)]

Match	[Add Conditions] ドロップダウンリストから目的の一致条件を選択します。次のオプションがあります。
	• アプリケーション
	• プロトコル
	• 送信元
	  • 位置情報
	  • IPv4 プレフィックス
	  • ポート
	• 接続先
	  • [FQDN]
	  • 位置情報
	  • IPv4 プレフィックス
	  • ポート

フィールド	説明
Action	目的のアクション条件を選択します。次のオプションがあります。 • Pass • Drop • Inspect • [Log Events]：検査アクションの統一されたロギング。ドロップダウンリストから [Advanced Inspection Profile] を選択します。
[User / User Group]	[User / User Group] サブポリシーを設定するには、アイデンティティサービスエンジンを有効にする必要があります。**[Administration]** > **[Integration Management]** > **[Identity Service Engine]**を使用して設定できます。

組み込みセキュリティの追加設定の指定

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policy Groups]**の順に選択し、[Embedded Security] を選択します。
2. リストからセキュリティポリシーを選択し、[Edit] をクリックして、次の詳細を入力します。
3. セキュリティポリシーの追加設定を指定するには、[Additional Settings] をクリックします。

フィールド	説明
[TCP SYN Flood Limit]	各宛先アドレスの毎秒SYNフラッドパケット数のしきい値を指定します。
[Max Incomplete]	ファイアウォールポリシーのタイムアウト制限を指定します。[Max Incomplete] タイムアウト制限は、ファイアウォールリソースを保護し、これらのリソースが使い果たされるのを防ぎます。
[TCP Limit]	デバイスで許可される最大TCPハーフオープンセッションを指定します。

フィールド	説明
[UDP Limit]	デバイスで許可される最大UDPハーフオープンセッションを指定します。
[ICMP Limit]	デバイスで許可される最大 ICMP ハーフオープンセッションを指定します。
[Audit Trail]	[Audit Trail] オプションを有効にします。このオプションは、検査アクションを持つルールにのみ適用されます。
[Unified Logging]	統合ログ機能を有効にします。
[Optimized Policy]	最適化ポリシーオプションを有効にします。
[Session Reclassify Allow]	ポリシー変更時にトラフィックの再分類を許可します。
[ICMP Unreachable Allow]	ICMP 到達不能パケットのパススルーを許可します。
[Advanced Inspection Profile]	デバイスレベルでグローバル詳細検査プロファイル（AIP）をアタッチします。検査対象のトラフィックに一致するデバイス内のすべてのルールが、詳細な検査プロファイルを使用して検査されます。

4. [Advanced Inspection Profile] ドロップダウンリストからプロファイルを選択するか、[Create New] をクリックします。

フィールド	説明
[Profile Name]	プロファイル名。
[Description]	プロファイルの説明です。
[Select an Intrusion Prevention]	デバイスで許可される最大TCPハーフオープンセッションを指定します。
[UDP Limit]	デバイスで許可される最大UDPハーフオープンセッションを指定します。
[ICMP Limit]	デバイスで許可される最大 ICMP ハーフオープンセッションを指定します。

フィールド	説明
[Audit Trail]	[Audit Trail] オプションを有効にします。このオプションは、検査アクションを持つルールにのみ適用されます。
[Unified Logging]	統合ログ機能を有効にします。
[Optimized Policy]	最適化ポリシーオプションを有効にします。
[Session Reclassify Allow]	ポリシー変更時にトラフィックの再分類を許可します。
[ICMP Unreachable Allow]	ICMP 到達不能パケットのパススルーを許可します。

5. [Select an Intrusion Prevention] ドロップダウンリストから侵入防御を選択するか、[Create New] をクリックします。

フィールド	説明
[Profile Name]	プロファイル名。名前は、最大 32 文字まで使用できます。
[Signature Set]	署名セットを指定します。次のオプションがあります。 • バランス • 接続性 • セキュリティ
[Inspection Mode]	検査モードを指定します。次のオプションがあります。 • 検知 • 保護
高度	

フィールド	説明
[Customer Signature Set]	新しいグローバルカスタム署名を追加するために、カスタマー署名セットを有効にします。[Add New Global Custom Signature] ウィンドウで、[Download From] でダウンロード元を次のオプションから選択します。 • リモート サーバ（Remote Server） • ローカル サーバ（非推奨）
[Select an Signature Allow List]	許可署名リストを選択するか、[Create New] を選択して新しい IPS 署名リストを作成します。
[Alert Log Level]	アラートログレベルを選択します。 • エラー • 緊急 • アラート • 深刻 • 警告 • 通知 • 情報 • デバッグ

6. [Add] をクリックします。
7. [Select an Advanced Malware Protection] ドロップダウンリストから高度なマルウェア保護プロファイルを選択するか、[Create New] をクリックします。

フィールド	説明
[Profile Name]	プロファイル名。名前は、最大 32 文字まで使用できます。
[Select AMP Cloud Region]	AMP クラウドリージョンを選択します。次のオプションがあります。 • NAM • EU • APJC

フィールド	説明
[Inspection Mode]	検査モードを指定します。次のオプションがあります。 • 検知 • 保護
[Alert Log Level]	アラートログレベルを選択します。 • 深刻 • 警告 • 情報
[File Analaysis]	ファイル分析を有効にします。
[Select TG Cloud Region]	ドロップダウンリストからクラウドリージョンを選択します。次のオプションがあります。 • NAM • EU
[Alert Log Level]	アラートログレベルを選択します。 • 深刻 • 警告 • 情報

フィールド	説明
[Select one or more file types]	ドロップダウンリストから 1 つ以上のファイルタイプを選択します。 • すべて（All） • pdf • [ms-exe] • [new-office] • rtf • mdb • [mscab] • [msole2] • [wri] • [xlw] • flv • swf

8. [Add] をクリックします。
9. [URL Filter] ドロップダウンリストから URL フィルタを選択するか、[Create New] を選択して新しいフィルタを作成します。

フィールド	説明
[Profile Name]	プロファイル名。名前は、最大 32 文字まで使用できます。
[Web Category]	ドロップダウンリストから Web カテゴリを選択します。次のオプションがあります。 • ブロック（Block） • 許可（Allow）
[Select one or more web categories]	ドロップダウンリストから 1 つ以上の Web カテゴリを選択します。オプションは、[abortion]、[abused-drugs] などです。

フィールド	説明
Web Reputation	ドロップダウンリストからWebレピュテーションを選択します。レピュテーションのオプションは、次のとおりです。 • 高リスク • 不審 • 中リスク • 低リスク • 高信頼性
高度	
[Select allow url list]	許可URLリストを選択するか、[Create New] を選択して新しい許可URLリストを作成します。
[Select block url list]	ブロックURLリストを選択するか、[Create New] を選択して新しいブロックURLリストを作成します。
[Block Page Server]	ドロップダウンリストからブロックページサーバーを選択します。次のオプションがあります。 • [Block Page Content] • [Redirect URL]：リダイレクトURLを指定します。
[Alerts And Logs]	ドロップダウンリストから1つ以上のファイルタイプを選択します。 • ブロックリスト • 許可リスト • レピュテーション/カテゴリ

10. [Add] をクリックします。
11. [TLS Action] を選択します。

フィールド	説明
[TLS Action]	ドロップダウンリストからWebカテゴリを選択します。次のオプションがあります。 • 復号（Decrypt） • パススルー（Pass Through） • [復号しない（Do not Decrypt）]
[Select an TLS/SSL Decryption]	ドロップダウンリストからTLS/SSL復号プロファイルを選択するか、[Create New] を選択して新しいプロファイルを作成します。

セキュアサービスエッジの設定

はじめる前に

[Administration] > **[Settings]** > **[Cloud Credentials]**から Cisco SSE ログイン情報を作成します。

セキュアサービスエッジの設定

[SSE Provider] を選択します。次のオプションがあります。

- Cisco Secure Access

トラフィックの設定

自動トンネルの作成中に、Cisco SD-WAN Manager は、フェールオーバーパラメータのデフォルト値を使用してデフォルトのトラッカーエンドポイントを作成し、アタッチします。ただし、要件に合ったフェールオーバーパラメータを使用してカスタマイズされたトラッカーを作成することもできます。

1. [Source IP Address] フィールドに、送信元の IP アドレスをサブネットマスクとともに入力します。
2. [Add Tracker] をクリックします。
3. [Add Tracker] ポップアップウィンドウで、次のように設定します。

表 *2:* トラッカーパラメータ

フィールド	説明
[Name]	トラッカーの名前。名前には 128 文字以内の英数字を使用できます。

フィールド	説明
[API url of endpoint]	トンネルの Secure Service Edge エンドポイントの API URL を指定します。 デフォルト：service.sig.umbrella.com
[Threshold]	設定されたエンドポイントがダウンしていることを宣言する前に、プローブが応答を返すまでの待機時間を入力します。 範囲： 100 ー 1000 ミリ秒 デフォルト： 300 ミリ秒
[Probe Interval]	設定されたエンドポイントのステータスを判断するためにプローブを送信する時間間隔を入力します。 範囲：20 ー 600 秒 デフォルト：60 秒
Multiplier（乗数）	トンネルがアップまたはダウンしていると判断する前にプローブを再送信する回数を入力します。 範囲：1 ～ 10 デフォルト：3

4. [Add] をクリックします。

トンネルの設定

トンネルを作成するには、[Configuration] をクリックして、次の手順を実行します。

1. [Add Tunnel] をクリックします。
2. [Add Tunnel] ポップアップウィンドウの [Basic Settings] で、次のように設定します。

表 *3*：基本設定

フィールド	説明
Tunnel Type	• Cisco Secure Access：（読み取り専用）**ipsec**
[Interface Name (1..255)]	インターフェイスの名前。
Description	インターフェイスの説明を入力します。
Tracker	デフォルトでは、トンネルの状態を監視するトラッカーがアタッチされています。

フィールド	説明
Tunnel Source Interface	トンネルの送信元インターフェイスの名前。このインターフェイスは出力インターフェイスである必要があります。通常はインターネット側のインターフェイスです。トンネル送信元インターフェイスはループバックをサポートします。
[Data-Center]	プライマリデータセンターの場合は [Primary] をクリックし、セカンダリデータセンターの場合は [Secondary] をクリックします。プライマリデータセンターへのトンネルはアクティブトンネルとして機能し、セカンダリデータセンターへのトンネルはバックアップトンネルとして機能します。
高度なオプション（オプション）	
Shutdown	オプションボタンをクリックしてこのオプションを有効にします。 デフォルト：無効
[Enable Tracker]	オプションボタンをクリックしてこのオプションを有効にします。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：576 ～ 2000 バイト デフォルト：1400 バイト
TCP MSS	TPC SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：500 ～ 1460 バイト デフォルト：なし
DPD Interval	インターネットキーエクスチェンジ（IKE）が接続で Hello パケットを送信する間隔を指定します。 範囲：10 ～ 3600 秒 デフォルト：10

フィールド	説明
DPD Retries	ピアからデッドピア検出（DPD）再試行メッセージの応答がない場合に、DPD再試行メッセージを送信する間隔を秒単位で指定します。 ピアがDPDメッセージに応答しなかった場合、ルータは状態を変更し、DPD 再試行メッセージを送信します。このメッセージは、より速い再試行間隔（DPD 再試行間の秒数）で送信されます。デフォルトで、DPD リトライ メッセージは2秒ごとに送信されます。5回の DPD 再試行メッセージに応答がない場合、トンネルはダウンとしてマークされます。 範囲：2 ～ 60 秒 デフォルト：3
IKE	
[IKE Rekey Interval]	IKE キーを更新する間隔を指定します。 範囲：3600 ～ 1209600 秒（1 時間～ 14 日） デフォルト：14400 秒
IKE Cipher Suite	IKE キー交換中に使用する認証と暗号化のタイプを指定します。 次のいずれかを選択します。 • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 デフォルト：AES 256 CBC SHA1
IKE Diffie-Hellman Group	IKEv1 または IKEv2 のいずれかで、IKE キー交換で使用する Diffie-Hellman グループを指定します。
IPSec	
IPsec Rekey Interval	IPSec キーを更新する間隔を指定します。 範囲：3600 ～ 1209600 秒（1 時間～ 14 日） デフォルト：3600 秒

フィールド	説明
[IPsec Replay Window]	IPsec トンネルのリプレイウィンドウサイズを指定します。 オプション：64、128、256、512、1024、2048、4096 パケット。 デフォルト：512
IPsec Cipher Suite	IPsec トンネルで使用する認証と暗号化を指定します。 次のオプションがあります。 • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM デフォルト：AEM 256 GCM
Perfect Forward Secrecy	IPSec トンネルで使用する Perfect Forward Secrecy（PFS）設定を指定します。次の Diffie-Hellman 素数係数グループのいずれかを選択します。 • グループ 2 1024 ビット係数 • グループ 14 2048 ビット係数 • グループ 15 3072 ビット係数 • グループ 16 4096 ビット係数 • なし：PFS を無効にします

3. [Add] をクリックします。

Cisco Secure Access にのみ適用されます。

[Region]：リージョンを選択すると、プライマリリージョンとセカンダリリージョンのペアが選択されます。Cisco Secure Service Edge が提供するプライマリリージョンをドロップダウンリストから選択すると、Cisco SD-WAN Manager でセカンダリリージョンが自動的に選択されます。ユニキャスト IP アドレスを持つプライマリリージョンに到達できない場合は、ユニキャスト IP アドレスを持つセカンダリリージョンに到達できます。その逆も同様です。Cisco Secure Access は、両方のリージョンが常に到達可能であることを保証します。

（注） HTTPS に接続してパブリック IP アドレスを取得するデバイスに DNS サーバーを設定できます。HTTPS の送信元インターフェイスを設定するには、Cisco SD-WAN Manager で **ip http client source-interface** コマンドを使用します。

ハイ アベイラビリティの設定

アクティブトンネルとバックアップトンネルを指定して、トンネル間でトラフィックを分散するには、[High Availability] をクリックして、次の手順を実行します。

1. [Add Interface Pair] をクリックします。
2. [Add Interface Pair] ポップアップウィンドウで、次のように設定します。

フィールド	説明
Active Interface	プライマリデータセンターに接続するトンネルを選択します。
[Active Interface Weight]	ロードバランシングの重み付け（重み付けの範囲：1 ～ 255）を入力します。 ロードバランシングは、複数のトンネル間でトラフィックを分散し、ネットワーク帯域幅を増やすのに役立ちます。両方のトンネルに同じ重み付けを入力すると、トンネル全体で ECMP ロードバランシングを実現できます。ただし、トンネルに高い重みを入力すると、そのトンネルのトラフィックフローの優先順位が高くなります。 たとえば、2 つのアクティブトンネルを設定する際、最初のトンネルの重み付けを 10 に設定し、2 番目のトンネルの重み付けを 20 に設定すると、トラフィックはトンネル間で 10:20 の比率で負荷分散されます。
[Backup Interface]	バックアップトンネルを指定するには、セカンダリデータセンターに接続するトンネルを選択します。 バックアップトンネルの指定を省略するには、[None] を選択します。

フィールド	説明
[Backup Interface Weight]	ロードバランシングの重み付け（重み付けの範囲：1 ～ 255）を入力します。 ロードバランシングは、複数のトンネル間でトラフィックを分散し、ネットワーク帯域幅を増やすのに役立ちます。同じ重み付けを入力すると、トンネル全体で ECMP ロードバランシングを実現できます。ただし、トンネルに高い重みを入力すると、そのトンネルのトラフィックフローの優先順位が高くなります。 たとえば、2 つのバックアップトンネルを設定する際、最初のトンネルの重み付けを 10 に設定し、2 番目のトンネルの重み付けを 20 に設定すると、トラフィックはトンネル間で 10:20 の比率で負荷分散されます。

3. [Add] をクリックします。

DNS セキュリティの設定

Cisco Umbrella 統合機能では、デバイスを介して DNS サーバーに送信されるドメインネームシステム（DNS）クエリを検証して、クラウドベースのセキュリティサービスを有効にすることができます。セキュリティ管理者は、完全修飾ドメイン名（FQDN）へのトラフィックを許可または拒否するポリシーを Cisco Umbrella ポータルに設定します。ルータは、ネットワークエッジの DNS フォワーダとして機能し、DNS トラフィックを透過的にキャッチして Cisco Umbrella クラウドに DNS クエリを転送します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policy Groups]** > **[DNS Security]** の順に選択します。
2. [Add DNS Security Policy] をクリックします。

フィールド	説明
[Add DNS Security Policy]	[Add DNS Security Policy] ドロップダウンリストから [Create New] を選択して、新しい [DNS Security Policy] のポリシーを作成します。
[Create New]	ドメインネームシステム（DNS）セキュリティポリシー ウィザードを表示します。
Policy Name	ポリシーの名前を入力します。
[Umbrella Registration Status]	API トークン設定のステータスを表示します。

フィールド	説明
[Manage Umbrella Registration]	[Manage Umbrella Registration] をクリックして Cisco Umbrella 登録キーおよびシークレットを追加します。DNS では、固有のネットワークデバイスキーが使用されます。 • [Organization ID] に組織 ID を入力します • [Registration Key] に登録キーを入力します。 • [Secret] にシークレットを入力します。 Cisco Umbrella のログイン情報は、**[Administration]** > **[Settings]** > **[Cloud Provider]** から編集できます。
[Match All VPN]	[Match All VPN] をクリックして、使用可能なすべての VPN に対して同じ設定を維持します。
[Custom VPN Configuration]	[Custom VPN Configuration] を選択して、特定の VPN を入力します。
[Local Domain Bypass List]	ドメインバイパスを選択します。
[DNS Server IP]	次のオプションから [DNS Server IP] を設定します。 • [Umbrella Default] • [Custom DNS]
DNSCrypt	DNSCrypt を有効または無効にします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。