SonicOS 7

プロファイル オブジェクト

管理者ガイド

SONICWALL®

目次

1

エンドポイント セキュリティ

「エンドポイント セキュリティ」では、製品購読とライセンス済みセキュリティ製品のログを一か所で管理できます。セキュリティ製品には、キャプチャ クライアント、コンテンツ フィルタ、侵入防御、アプリケーション制御、ボットネット/地域 IP フィルタ、ゲートウェイ アンチウイルス/アンチスパイウェア/キャプチャ ATP などがあります。

有効になっている場合、Capture Clientはクラウド サンドボックス ファイル テスト、包括的なレポート機能、およびエンドポイント保護の適用を利用しながら、使いやすくアクション可能な情報とレポートによりクライアント セキュリティを一貫して実現します。

エンドポイント セキュリティは、端末がどこにあるかを問わずエンドポイントを保護し、マルウェアの侵入を阻止しながらアクセス ルールとコンテンツ ルールを適用します。

エンドポイント セキュリティの設定については、SonicOS の「*ポリシー > エンドポイント セキュリティ*」セクションを参照してください。

既定のエンドポイント セキュリティ プロファイルである「**エンドポイント セキュリティの既定プロファイル**」は、SonicOS によって作成されます。このエンドポイント セキュリティ プロファイルは、構成および編集は可能ですが、削除することはできません。

エンドポイント セキュリティ プロファイルを追加するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > エンドポイント セキュリティ**」ページに移動します。
2. ページ上部の**追加**アイコンをクリックします。
3. 「**名前**」フィールドにエンドポイント セキュリティ プロファイルの名前を入力します。
4. 「**ゲスト エンドポイント セキュリティ サービスをバイパスする**」オプションをオンにして有効にします。このオプションを有効にすると、一致するゾーンでゲスト サービスが有効な場合にエンドポイント セキュリティのゲスト確認がバイパスされます。
5. 「**キャプチャ クライアント エンドポイント セキュリティ**」オプションをオンにして有効にします。
6. 「**保存**」をクリックします。エンドポイント セキュリティ プロファイルが作成されます。

エンドポイント セキュリティ プロファイルを削除するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > エンドポイント セキュリティ**」ページに移動します。
2. 削除したいエンドポイント セキュリティ プロファイルのチェックボックスを選択し、ページ上部の**削除**アイコンをクリックします。

   または

   エンドポイント セキュリティ プロファイルにマウス カーソルを重ね、**削除**アイコンをクリックします。

2

帯域幅

帯域幅管理の設定は、トラフィック等級に対する帯域幅制限を指定するポリシーに基づいています。完全な帯域幅管理ポリシーは、分類基準と帯域幅ルールという 2 つの部分で構成されます。

分類基準は、優先順位、保証帯域幅、最大帯域幅など、実際のパラメータを指定し、帯域幅オブジェクト内で構成されます。分類基準は、具体的な基準との照合によってパケットの識別とトラフィック等級への分類を行います。

帯域幅オブジェクトの設定

帯域幅オブジェクトを追加または構成するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > 帯域幅**」ページに移動します。
2. 以下のいずれかを実行します。
   - **追加**アイコンをクリックして、新しい帯域幅オブジェクトを作成します。
   - 編集する帯域幅オブジェクトにマウス カーソルを重ね、**編集**アイコンをクリックします。

   次のダイアログ画面が表示されます。

3. 「**名前**」フィールドに、帯域幅オブジェクトの説明的な名前を入力します。

4. 「**保証帯域幅**」フィールドに、この帯域幅オブジェクトがあるトラフィックへの提供を保証する帯域幅の量を入力します。数字を入力し、ドロップダウンリストから Kbps（キロビット/秒）または Mbps（メガビット/秒）レートを選択します。
5. 「**最大帯域幅**」フィールドに、この帯域幅オブジェクトがあるトラフィックに提供する帯域幅の最大量を入力します。数字を入力し、ドロップダウンリストから Kbps または Mbps レートを選択します。

   ⓘ **補足:** 複数のトラフィック等級が共有された帯域幅をめぐって競合している場合、実際に割り当てられる帯域幅はこの値よりも少なくなることがあります。
6. 「**トラフィック優先順位**」ドロップダウン リストで、あるトラフィック等級に対してこの帯域幅オブジェクトが付与する優先順位を選択します。最高の優先順位は「**0（リアルタイム）**」で、これが既定値です。最低の優先順位は「**7（最低）**」です。

   複数のトラフィック等級が共有された帯域幅をめぐって競合している場合は、優先順位が指向の等級に優先権が与えられます。
7. 「**違反動作**」ドロップダウン リストで、トラフィックが最大帯域幅の設定値を上回った場合にこの帯域幅オブジェクトが実行する動作を選択します。
   - **遅延** – 過剰なトラフィック パケットをキューに登録し、送信可能になった時点で送信することを示します（既定で選択されています）。
   - **破棄** – 過剰なトラフィック パケットが直ちに破棄されることを示します。
8. 「**コメント**」フィールドに、この帯域幅オブジェクトに対するコメントまたは説明のテキストを入力します。
9. 「**基本**」タブを選択します。

10. 必要に応じて、「**IP 毎帯域幅管理を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。「最大帯域幅」フィールドが有効になります。

    IP 毎帯域幅管理を有効にする が有効になっている場合、最大の基本帯域幅の設定は親のトラフィック等級の下にある個々の IP に適用されます。
11. 「**最大帯域幅**」の値を入力します（数字）。
12. 関連するドロップダウン リストで、「**Kbps**」または「**Mbps**」のいずれかの単位を選択します。
13. 「**保存**」をクリックします。

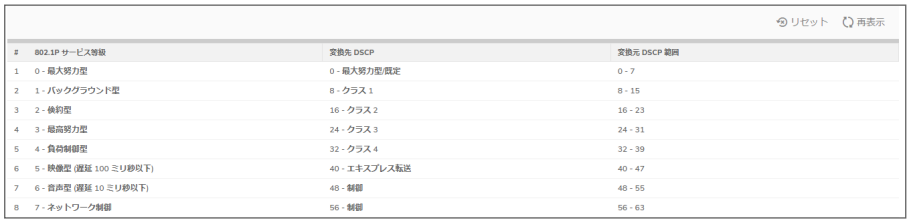
ⓘ **補足:** アクセス ルールに帯域幅オブジェクトを設定する場合は、「**ポリシー > ルールとポリシー > アクセス ルール > ルールの追加**」の章の「*高度な帯域幅管理による帯域幅管理設定の構成*」および「*グローバル帯域幅管理による帯域幅管理設定の構成*」を参照してください。

3

サービス品質 (QoS) 級割

サービス品質 (QoS) とは、より予測可能なネットワークの動作とパフォーマンスを提供するために使用される多様な方式を指します。予測可能性は、VoIP (Voice over IP) やマルチメディア コンテンツなどの特定の種類のアプリケーションはもちろん、発注処理やクレジット カード決済などのビジネス アプリケーションにとって、特に重要です。帯域幅量をいくら調整しても十分な予測可能性を提供できません。なぜなら、帯域幅をどんなに増やしても、ネットワークでは任意の時点でその容量まで使い果たされる結果になるからです。QoS を正しく構成し実装すると、トラフィック管理を大幅に改善し、高いレベルのネットワーク サービスを保証することが可能になります。本章では、SonicOS ユーザ インターフェースのマッピング テーブルを示します。このテーブルでは、管理者がマッピング設定に変更を加えることができます。その後、ネットワーク上で QoS を向上させるために用いられるいくつかの技法を詳しく説明します。

ユーザ インターフェースを使用すると、管理者は外部システム全体の QoS サービス用に 802.1p を DSCP 級割にマッピングする設定を行うことができます。下に示すテーブルは、相互の関係を示しており、鉛筆アイコンは設定を表します。任意の行のアイコンを選択すると、ダイアログが開き、マッピング テーブルへの変更が必要であるかどうかを選択するためのオプションが表示されます。選択肢はドロップダウン メニューで表示されます。「**リセット**」をクリックすると、変更が適用されます。



トピック:

- 分類
- 級割
- 制限
- 802.1p と DSCP QoS
- 用語集

分類

分類は、管理が必要なトラフィックを識別できるようになるための最初のステップとして必要です。SonicOS は、トラフィックの分類へのインターフェースとしてアクセス ルールを使用します。これにより、アドレス オブジェクト、サービス オブジェクト、スケジュール オブジェクトの要素の組み合わせを使用した、きめの細かい制御が提供されます。分類基準は、"**すべての HTTP トラフィック**" のように大まかに設定することも、"**毎週水曜日午前 2:12 のホスト A からサーバ B への SSH トラフィック**" のように詳細に設定することもできます。

SonicWall ネットワーク セキュリティ装置では、業界標準の外部の CoS 識別子、DSCP、802.1p を認識、割付、編集、生成することができます。詳細については、「802.1p と DSCP QoS」を参照してください。

識別または分類されると、管理可能になります。管理は、ネットワークが完全な自律システムである限り、完璧に効果的な SonicOS の帯域幅管理 (BWM) により内部的に実行されます。未知の構成の外部ネットワーク インフラ、または、帯域幅を争う他のホスト (例えば、インターネット) などのような、外部または中間の要素が導入されると、保証と予測を提供する能力は低下します。言い換えれば、ネットワークのエンドポイントとその間にあるものがすべて管理内にある限りは、帯域幅管理は構成した通りに機能します。外部の要素が導入されると、帯域幅管理の精度と有効性は低下し始めます。

しかし、すべてが失われるわけではありません。SonicOS がトラフィックを分類した後、トラフィックに**タグ**を付けて、CoS タグを遵守できる特定の外部システムにこの分類を通知できます。その結果、これらの外部システムも QoS の提供に関与することができます。

ⓘ **補足:** 多くのサービス プロバイダは、802.1p や DSCP などの CoS タグをサポートしていません。また、標準的な設定のほとんどのネットワーク デバイスは、802.1p タグを認識できずに、タグ付けされたトラフィックを破棄します。
DSCP は互換性の問題を発生しませんが、多くのサービス プロバイダは、コード ポイントに関係なく、DSCP タグを単に取り除くか、無視します。
会社のネットワークまたはサービス プロバイダのネットワーク上で 802.1p または DSCP 級割を使用する場合は、これらの方式がサポートされていることを最初に確認する必要があります。内部ネットワーク デバイスが CoS 優先級割をサポートできること、およびこのサポートを提供するために正しく構成されていることを確認します。サービス プロバイダに確認します (CoS 方式を使用したQoS サポートを有償で提供しているところもあります)。

級割

トラフィックを分類した後、QoS 対応外部システム (例えば、プレミアム サービス プロバイダのインフラストラクチャかプライベート WAN 上で利用可能な、CoS 対応のスイッチやルータ) により処理されることになっている場合、トラフィックにタグを付けて、外部システムが分類を利用して適切な処理とホップ単位動作 (PHB) を提供できるようにする必要があります。

元々、これは RFC791 の 3 つの優先順位ビットと RFC1394 の ToS (サービス タイプ) フィールドとともに IP 層 (第 3 層) で試みられました。これは、歴史を通じて、総勢 17 名が使用しました。後継の RFC2474 では、より実用的で広範囲にわたって使用することのできる、64 個までの分類とユーザ定義等級を提供する DSCP (Differentiated Services Code Point) が採用されています。DSCP は、RFC2598 (専用線の動作を提供するための緊急転送) と RFC2697 (等級内部での保証転送レベル。金、銀、銅レベルとしても知られている) によりさらに拡張されました。

DSCP は、非互換の危険性がないので、パブリック ネットワークを通過するトラフィックのための安全な級割方式です。最悪の場合、パスに沿ったホップでは、DSCP タグが無視されるか除去される可能性がありますが、パケットの誤処理や破棄はほとんど発生しません。

CoS 級割のもう 1 つの一般的な方式は、IEEE 802.1P です。802.1P は、MAC 層（第 2 層）で動作し、実際には IEEE 802.1D 標準で定義されていますが、（同じ 16 ビット フィールドを共有して）IEEE 802.1Q VLAN 級割と密接に関連しています。DSCP とは異なり、802.1P は、802.1p 対応デバイスでのみ動作し、広く相互利用が可能であるわけではありません。さらに、802.1P は異なるパケット構造を持つので、広域ネットワークや、プライベート WAN をほとんど通過できません。それでもなお、802.1p は、音声および Video over IP ベンダーの間で、幅広い支持を得ています。そこで、ネットワークの境界（WAN リンクなど）を横断する 802.1P をサポートするためのソリューションが、**802.1P を DSCP へ割り付ける**形で導入されました。

802.1P の DSCP への割付では、パケットが安全に WAN リンクを通過できるようにするために、ある LAN からの 802.1P タグが SonicOS によって DSCP の値に割り付けられます。パケットがWAN または VPN の反対側に到着すると、受信側 SonicOS 装置により、DSCP タグが LAN で使用するために 802.1P タグに戻されます。詳細については、「802.1p と DSCP QoS」を参照してください。

制限

トラフィックは、利用可能な多くのポリシング、キューイング、シェイピングのどれかを使用して、制限（管理）することができます。SonicOS は、送信および受信帯域幅管理（BWM）による内部制限機能を提供します。SonicOS の帯域幅管理は、十分な帯域幅を持つ完全な自律プライベート ネットワークにとって完璧に効果的なソリューションですが、より未知の外部ネットワーク要素や、帯域幅の競合に遭遇した場合に、効果的でなくなることがあります。競合の問題については、「DSCP 級割: サンプル シナリオ」を参照してください。

トピック:

- QoS 対応ネットワークでのサイト間 VPN
- パブリック ネットワークでのサイト間 VPN

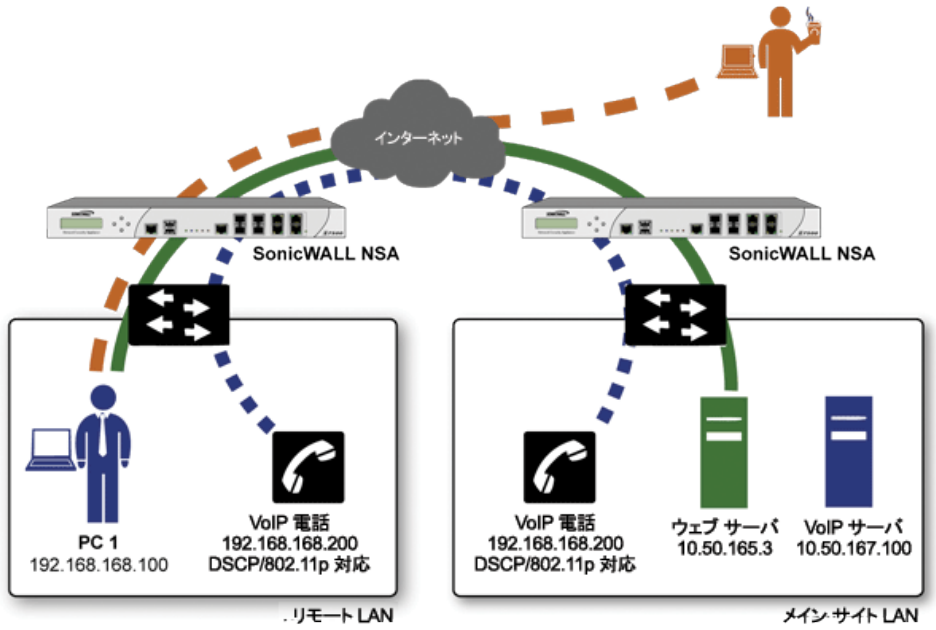
QoS 対応ネットワークでのサイト間 VPN

2 つのエンド ポイント間のネットワーク パスが QoS に対応している場合、SonicOS は、内部カプセル化パケットがトンネルの反対側で正常に解釈されるように DSCP タグを付けてることができます。さらに、外部 ESP カプセル化パケットに DSCP タグを付けて、通過ネットワークの各ホップでその等級が解釈および適用されるようにできるようにすることもできます。SonicOS は、通過ネットワークを安全に通過できるように、内部ネットワークで作成された 802.1p タグを DSCP タグに割り当てることができます。パケットが反対側に到着すると、受信側 SonicWall 装置は、DSCP タグを内部ネットワークで解釈および適用できるように 802.1p タグに逆変換できます。

パブリック ネットワークでのサイト間 VPN

SonicOS 統合帯域幅管理 は、両方のエンド ポイントで受信トラフィックと送信トラフィックを分類および制御できるので、VPN 接続ネットワーク間のトラフィックを管理するのに非常に効果的です。エンド ポイント間のネットワークが QoS に対応していない場合、すべての VPN ESP は等しく認識および処理されます。通常、これらの中間ネットワークまたはそのパスに対する制御は行われないため、QoS を完全に保証することは困難ですが、より予測可能な動作を提供するのに役立ちます。

パブリック ネットワークでのサイト間 VPN



VoIP トラフィック

ウェブ トラフィック

VoIP トラフィック

LAN -> VPN	DSCP: 48	802.11p: 6	受信	Gar. 30%	Max: 60%	Pri: 0
LAN -> VPN	DSCP: 48	802.11p: 6	送信	Gar. 30%	Max: 60%	Pri: 0
VPN -> LAN	DSCP: 48	802.11p: 6	受信	Gar. 30%	Max: 60%	Pri: 0
VPN -> LAN	DSCP: 48	802.11p: 6	送信	Gar. 30%	Max: 60%	Pri: 0

ウェブ トラフィック (HTTP、HTTPS、NNTP、TCP4662)

LAN -> VPN	DSCP: 8	802.11p: 1	受信	Gar. 5%	Max: 30%	Pri: 2
LAN -> VPN	DSCP: 8	802.11p: 1	送信	Gar. 5%	Max: 30%	Pri: 2
LAN -> WAN	DSCP: 0	802.11p: -	受信	Gar. 2%	Max: 30%	Pri: 7
LAN -> WAN	DSCP: 0	802.11p: -	送信	Gar. 2%	Max: 10%	Pri: 7

エンド ツー エンド QoS を提供するために、ビジネス クラスのサービス プロバイダは、彼らの IP ネットワーク上でトラフィックの制限サービスを提供するようになりました。通常、これらのサービスは、トラフィックの分類およびタグ付けに関して顧客の設備に依存します (一般に、DSCP などの標準の級割方式を使用します)。SonicOS は、分類後にトラフィックを DSCP 級割する機能に加え、外部ネットワークの横断と CoS の維持を可能にするための、802.1p タグを DSCP タグに割り付ける機能を備えています。VPN トラフィックの場合、SonicOS は、内部 (ペイロード) パケットだけでなく、外部 (カプセル化) パケットも同様に DSCP 級割できます。これにより、QoS 対応サービス プロバイダは、暗号化された VPN トラフィックに対しても QoS を提供できます。

サービス プロバイダによって採用されている実際の制限方式は各種ありますが、一般的に、トラフィックに優先順位を付けるための重み付け公平キューイング (WFQ) のような等級をベースとしたキューイング方式や、テールドロップやランダム初期検知などの輻輳を回避する方式が使用されています。

802.1p と DSCP QoS

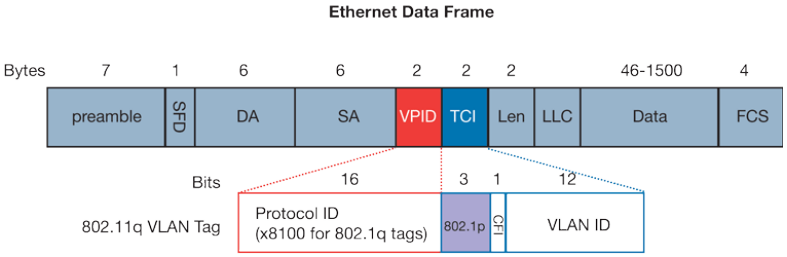
トピック:

- 802.1p の有効化
- DSCP 級割

802.1p の有効化

SonicOS では、QoS に対応する環境に参加している外部システムとの広い範囲での相互運用性を実現するために、第 2 層と第 3 層 CoS 方式をサポートしています。第 2 層の方式は、下図に示すように、フレームの優先順位を指定するために、イーサネット フレームのヘッダーに挿入された追加の 16 ビットのうちの 3 ビットを用いることのできる、IEEE 802.1p 標準です。

イーサネット データ フレーム



- **TPID**: TPID (Tag Protocol Identifier) は、バイト 12 から始まります (6 バイトの宛先アドレスと送信元アドレスの後)。2 バイトの長さで、タグ付けされたトラフィックは 0x8100 のイーサ種別を持ちます。
- **802.1p**: TCI (タグ制御情報 ― バイト 14 から始まり、2 バイトの長さ) の最初の 3 ビットは、ユーザ優先順位を定義します (8 つ (2 の 3 乗) の優先順位レベルを与えます)。IEEE 802.1p では、これらの 3 ビットのユーザ優先順位の処理を定義しています。
- **CFI**: CFI (Canonical Format Indicator) は、単一ビットフラグで、イーサネット スイッチの場合は常に 0 に設定されます。CFI は、イーサネット ネットワークとトークン リング ネットワークの間の互換性のために使用されます。イーサネット ポートで受信されたフレームの CFI が 1 に設定されている場合、そのフレームは、タグ付けされていないポート用なので転送してはいけません。
- **VLAN ID**: VLAN ID (バイト 14 のビット 5 から始まる) は、VLAN の ID です。12 ビットあり、4,096 (2 の 12 乗) の VLAN ID を表現することができます。4,096 の ID のうち、ID 0 が優先順位フレームの識別に使用され、ID4,095 (FFF) が予約されているので、最大 4,094 のVLAN を設定できます。

802.1p のサポートを開始するには、プロセスの 802.1p タグを持たせたいインターフェースで 802.1p 級割を有効にします。802.1p は、任意の SonicWall 装置のイーサネット インターフェースで有効にできます。

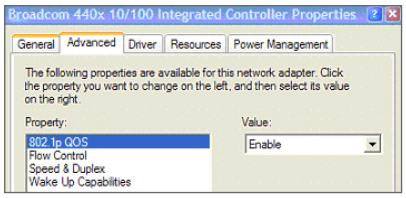
これらのタグの内部の 802.1p フィールドの動作は、アクセス ルールで制御することができます。既定の 802.1p アクセス ルール動作の「**なし**」は、特に構成しない限り、既存の 802.1p タグを 0 にリセットします (詳細は、「QoS 級割の管理」を参照)。

802.1p 級割を有効化すると、802.1p 対応ネットワーク デバイスにより生成された着信 802.1p タグをターゲット インターフェースが認識できるようになり、また、アクセス ルールによる制御としてターゲット インターフェースが 802.1p タグを生成することが可能になります。SonicOS により挿入された 802.1p タグを持つフレームは、VLAN ID 0 を持ちます。

802.1p タグは、アクセス ルールに従って挿入されるだけなので、インターフェース上で既定の設定で802.1p 級割を有効にしても、802.1p 非対応デバイスとの通信は中断されません。

802.1p の場合、この優先順位付け方式を使用したいネットワーク デバイスによる特定のサポートを必要とします。多くのボイスおよびビデオ オーバー IP デバイスは、802.1p のサポートを提供していますが、機能を有効化する必要があります。不確かな場合には、802.1p のサポートについて、装置の説明書を確認してください。同様に、多くのサーバとホストのネットワーク カード (NIC) は 802.1p をサポートする機能を持ちますが、通常この機能は既定で無効になっています。Win32 オペレーティング システムの場合、ネットワーク カードの「プロパティ」ページの「**詳細設**

定」ビューで 802.1p の設定を確認および構成することができます。カードが 802.1p をサポートしている場合、「**802.1p QoS**」、「**802.1p Support**」、「**802.1p QoS Packet Tagging**」のような項目が表示されます。

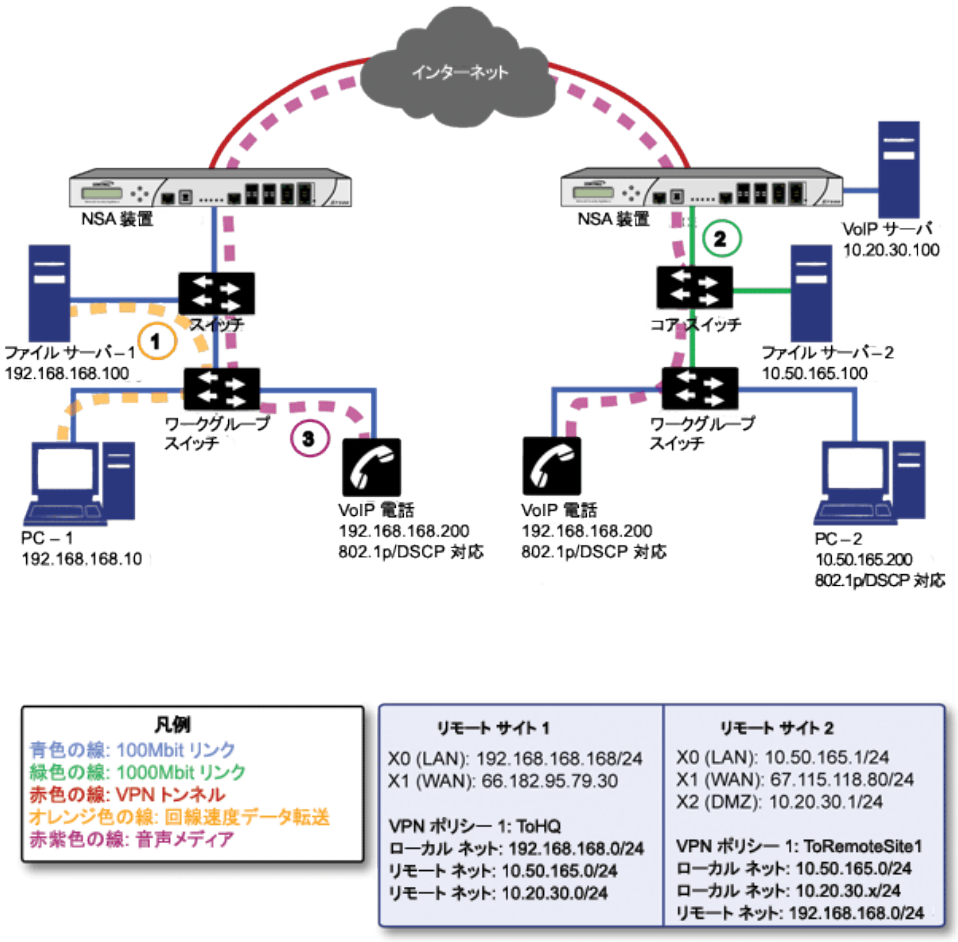


802.1p タグを処理するためには、ネットワーク インターフェースで機能が存在し有効にされている必要があります。これにより、ネットワーク インターフェースは、QoS 対応アプリケーションにより制御され、802.1p タグ付きのパケットを生成できます。既定では、一般的なネットワーク通信では、802.1p 非対応デバイスとの互換性を維持するためにタグは挿入されません。

ⓘ **補足:** 802.1p をサポートしていないネットワーク インターフェースは、802.1p のタグ付けされたトラフィックを処理できず、無視します。802.1p 級割を有効にするためのアクセス ルールを定義する場合は、ターゲット デバイスが 802.1p に対応することを確認してください。
また、(Ethereal 診断ツールを使用して) 802.1p 対応デバイス上でパケット監視を行う場合は、いくつかの 802.1p 対応デバイスでパケット監視内で 802.1p ヘッダーが表示されないことがある点にも注意してください。逆に言えば、802.1p 非対応デバイス上でパケット監視を行うと、ほとんど例外なくヘッダーが表示されますが、ホストはパケットを処理することができなくなります。

QoS 級割方式と DSCP 級割方式の間には潜在的な相互依存があるので、先へ進む前に、「DSCP 級割」について紹介し、相互依存が存在する理由について説明します。詳細については、「QoS 級割の管理」を参照してください。

DSCP 級割: サンプル シナリオ



上のシナリオで**リモート サイト 1** は、IPSec VPN により「メイン サイト」に接続されています。この企業は、プライベート VoIP シグナリング サーバをメイン サイトに配置して、内部で 802.1p/DSCP 対応 VoIP 電話システムを使用しています。メイン サイトでは、ギガビットとファスト イーサネットの混合した基盤を使用しています。一方、リモート サイト 1 では、すべてファスト イーサネットを使用しています。内部トラフィックの優先順位付けのために、両方のサイトで 802.1p 対応スイッチが使用されています。

1. リモート サイト 1 の PC–1 は、23 テラバイトのパワーポイント プレゼンテーションをファイル サーバ 1 へ送信しており、ワークグループ スイッチと上流スイッチとの間の 100 Mbps のリンクは完全に飽和状態になっています。
2. メイン サイトで、802.1p/DSCP 対応 VoIP 電話 (10.50.165.200) のユーザが、VoIP 電話 (192.168.168.200) のユーザに電話をかけます。呼び出し元の VoIP 電話の 802.1p によりトラフィックに優先順位タグ 6 (音声) が付けられ、また、DSCP によりトラフィックに 48 のタグが付けられます。
    a. コア スイッチとファイアウォールの間のリンクが VLAN の場合、スイッチによっては、ファイアウォールへ送信されるパケット内に、受信した 802.1p 優先順位タグを DSCP タグに加えて含めるものがあります (この動作はスイッチによって異なり、設定が可能な場合もあります)。
    b. コア スイッチとファイアウォールの間のリンクが VLAN でない場合、スイッチが 802.1p 優先順位タグを含める方法はありません。802.1p 優先順位は削除され、(DSCP タグのみを含む) パケットがファイアウォールに転送されます。

VPN/WAN リンクを経由してパケットを送信する場合、ファイアウォールでパケット内に DSCPタグを含めることができますが、802.1p タグを含めることはできません。これは、VoIP トラフィックのすべての優先順位情報を失う結果となります。なぜならば、パケットがリモート サイトに到着した際に、トラフィックの優先順位付けを行うための 802.1p MAC 層情報をスイッチが持たないからです。リモート サイト スイッチは、VoIP トラフィックを低優先順位のファイル転送と同じと見なします。リンクが飽和状態のため、VoIP フローは遅延し（パケットが破棄される場合もあります）、音質の低下を招く結果となります。

では、メイン サイト LAN からの重要な 802.1p 優先順位情報を VPN/WAN リンクを横断してリモート サイト LAN へと引き継ぐにはどうしたらよいのでしょうか。それには、QoS 割付を使用します。

QoS 割付は、第 2 層の 802.1p タグを第 3 層の DSCP タグに変換して、（割り付けられた形式で）802.1p タグが 802.1p 非対応リンクを安全に横断できるようにする機能です。パケットが配送のために次の 802.1p 対応セグメントに到着すると、QoS 割付機能により、DSCP が元の802.1p タグに変換され、第 2 層 QoS が利用できるようになります。

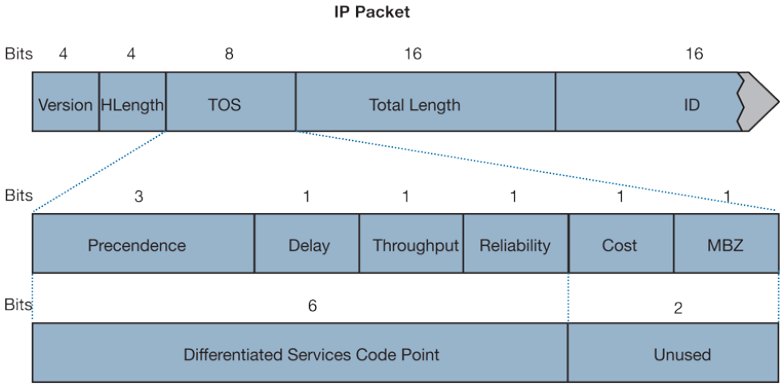
上記のシナリオでは、メイン サイトのファイアウォールで DSCP タグ（例えば、値 **48**）を VoIP パケットとカプセル化 ESP パケットに割り当てて、WAN にわたってレイヤ 3 QoS を適用します。この割り当ては、既存の DSCP タグを維持すること、または、802.1p タグから値を割り付けることにより発生します。VoIP パケットがリンクの反対側に到着すると、受信側 SonicWall によって逆の割付処理が行われます。すなわち、DSCP タグが元の 802.1p タグに割り付けられます。

3. リモート サイトの受信側 SonicWall ネットワーク セキュリティ装置は、DSCP タグ範囲 48～55 を 802.1p タグ 6 に割り付けるように構成されています。ファイアウォールから発信されるパケットは、802.1p タグ 6 を運びます。スイッチは、それが音声トラフィックであると認識し、ファイル転送よりも優先して、リンクが飽和した場合でも QoS を保証します。

DSCP 級割

DSCP（Differentiated Services Code Point）級割では、IP ヘッダー内の 8 ビットの ToS フィールドのうちの 6 ビットを使用して、最大 64 のトラフィックの等級（またはコード ポイント）を提供します。DSCP は第 3 層の級割方式なので、802.1p の級割であったような互換性についての心配はありません。DSCP をサポートしていないデバイスでは単にタグが無視されます。最悪の場合でも、タグの値が 0 にリセットされるだけです。

DSCP 級割: IP パケット



上の画像は、IP パケットと、ヘッダーの ToS 部分を拡大した図です。ToS ビットは、元々は優先順位とToS（遅延、スループット、信頼性、コスト）設定のために使用されていましたが、その後、より多用途の DSCP 設定用に RFC2474 で再定義されました。

下の表に、一般的に使用されているコード ポイントと、従来の優先順位および ToS 設定に対する割り当てを示します。

DSCP 級割: 一般的に使用されるコード ポイント

DSCP	DSCP の説明	従来の IP 優先順位	従来の IP ToS (D、T、R)
0	最大努力型	0 (通常 — 000)	–
8	等級 1	1 (優先順位 — 001)	–
10	等級 1、金 (AF11)	1 (優先順位 — 001)	T
12	等級 2、銀 (AF12)	1 (優先順位 — 001)	D
14	等級 1、銅 (AF13)	1 (優先順位 — 001)	D、T
16	等級 2	2 (即時 — 010)	–
18	等級 2、金 (AF21)	2 (即時 — 010)	T
20	等級 2、銀 (AF22)	2 (即時 — 010)	D
22	等級 2、銅 (AF23)	2 (即時 — 010)	D、T
24	等級 3	3 (フラッシュ — 011)	–
26	等級 3、金 (AF31)	3 (フラッシュ — 011)	T
27	等級 3、銀 (AF32)	3 (フラッシュ — 011)	D
30	等級 3、銅 (AF33)	3 (フラッシュ — 011)	D、T
32	等級 4	4 (フラッシュ オーバライド — 100)	–
34	等級 4、金 (AF41)	4 (フラッシュ オーバライド — 100)	T
36	等級 4、銀 (AF42)	4 (フラッシュ オーバライド — 100)	D
38	等級 4、銅 (AF43)	4 (フラッシュ オーバライド — 100)	D、T
40	エキスプレス転送	5 (CRITIC/ECP – 101)	–
46	緊急転送 (EF)	5 (CRITIC/ECP – 101)	D、T
48	制御	6 (インターネット制御用 — 110)	–
56	制御	7 (ネットワーク制御用 — 111)	–

ⓘ | **ヒント:** ECP: Elliptic Curve Group (楕円曲線群)

DSCP 級割は、すべてのインターフェースの発着信トラフィックに対して、ゾーンのタイプを問わず、例外なく実行することができます。DSCP 級割は、「**QoS**」ビューのアクセス ルールで制御され、802.1p 級割と併用して使用できます。また、SonicOS 内部の帯域幅管理でも使用されます。

トピック:

- DSCP 級割と混在 VPN トラフィック
- 802.1p CoS 4 – 負荷制御型の構成
- QoS 割付
- QoS 級割の管理

DSCP 級割と混在 VPN トラフィック

数ある安全対策と特性の中で、IPSec VPN では、ESP ヘッダーに追加される単調に増加するシーケンス番号に基づくアンチリプレイ機構を採用しました。シーケンス番号が重複するパケットは、シーケンス基準を満たさないという

理由で破棄されます。このような基準の 1 つは、到着順序の異なるパケットの処理を管理します。SonicOS では、64 パケット分のリプレイ ウィンドウが提供されます。すなわち、Security Association (SA) の ESP パケットが 64 パケットを超えて遅延した場合、パケットは破棄されます。

DSCP 級割を使用して VPN を横断するトラフィックに第 3 層 QoS を提供する場合は、この点を考慮する必要があります。さまざまなトラフィックが転送されている VPN トンネルがあるとします。高優先順位の DSCP タグが付けられたトラフィック (VoIP など)、低優先順位の DSCP タグが付けられたトラフィック、タグを付けられていないトラフィック、最大努力型 (FTP など) の DSCP タグが付けられたトラフィックが混在する場合、サービス プロバイダは、最大努力型の ESP パケットよりも、高優先順位の ESP パケットの処理と配送を最も優先します。その結果、トラフィックの条件によっては、最大努力型のパケットが 64 パケットを超えて遅延し、受信側の SonicWall のアンチリプレイ防御によりパケットが破棄される場合があります。

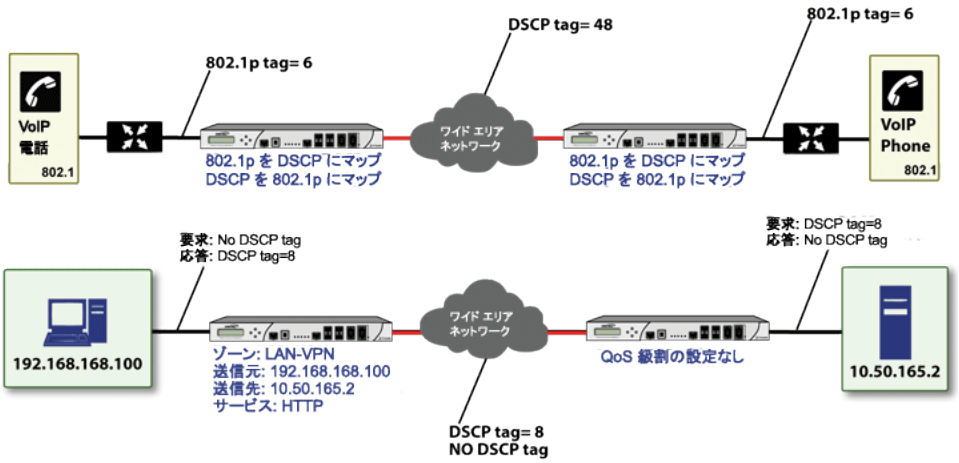
そのような現象が発生する場合 (例えば、低優先順位のトラフィックの過度の再送が発生する場合) は、高優先順位と低優先順位のトラフィック用に別個の VPN ポリシーを作成することをお勧めします。これを簡単に実現するには、高優先順位のホスト (例えば、VoIP ネットワーク) を、それら自身のサブネットに配置します。

802.1p CoS 4 – 負荷制御型の構成

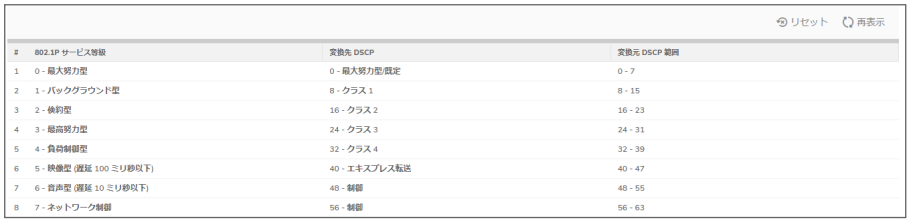
DSCP タグ 15 を既定の 802.1p 割付の 1 から 802.1p 割付の 2 に変更する場合、割付範囲は重複できないので、2 つの手順が必要です。範囲を重複して割付を行おうとすると、「DSCP 範囲は、既に存在するか、他の範囲と重複しています。」というエラーが発生します。最初に、802.1p CoS 1 に対する現在の終了範囲割付から 15 を削除し (802.1p CoS 1 の終了範囲割付を DSCP 14 に変更し)、次に 802.1p CoS 2 の開始範囲割付に DSCP 15 を割り当てます。

QoS 割付

QoS 割付の第 1 の目的は、WAN リンクを経由する送信の前に 802.1p タグと対応する DSCP タグを割り付け、リンクの反対側に到着したときに DSCP から 802.1p に割り付け戻すことにより、802.1p 非対応リンク (WAN リンクなど) を横断して 802.1p タグを維持できるようにすることにあります (下の図を参照)。



ⓘ **補足:** 割付は、アクセス ルールの「QoS」ビューの動作として、「**参照**」を割り当てるまで行われません。割付テーブルは、アクセス ルールの参照の方針によって使用される対応を定義しているだけです。



例えば、既定のテーブルに従った場合、値が 2 の 802.1p タグは、送信用に 16 という DSCP 値が割り当てられ、値が 43 の DSCP タグは、受信用に 5 という 802.1p 値が割り当てられます。

これらの割付は再構成できます。802.1p タグ 4 の送信割付を既定の DSCP 値の 32 から 43 に変更したい場合、4 の構成アイコンをクリックし、ドロップダウン ボックスから新しい「変換先 DSCP」の値を選択します。

「**リセット**」オプションをクリックすることにより、既定の割付に戻すことができます。

QoS 級割の管理

QoS 級割の構成は、「**ポリシー**>**ルールとポリシー**>**アクセス ルール**>**ルールの追加**」ページの「**ルールの追加/編集**」ダイアログの「**トラフィック シェーピング**」タブで行います。

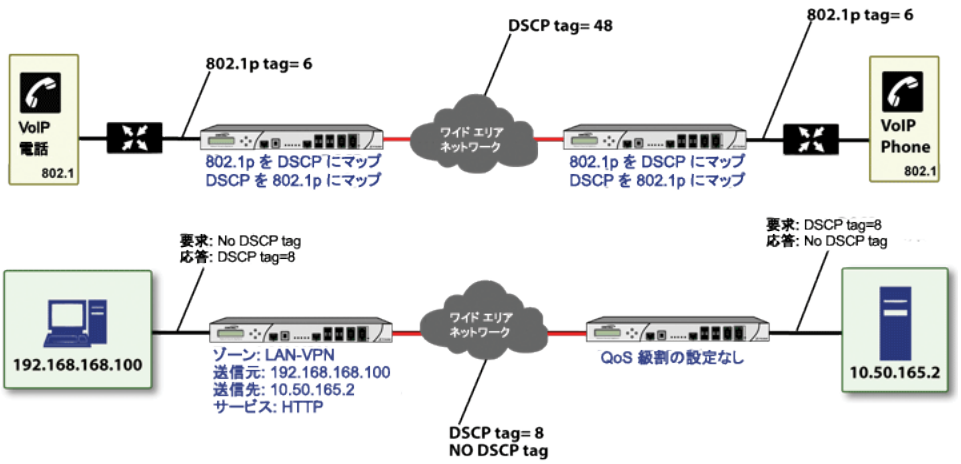
SonicOS のアクセス ルールで管理される 802.1p および DSCP 級割では、「**なし**」、「**維持**」、「**指定**」、「**参照**」の 4 つの方針が提供されます。DSCP の既定の方針は「**維持**」で、802.1p の既定の方針は「**なし**」です。

下の表では、両方の級割方式での各方針の動作について説明します。

動作	802.1p（第 2 層 CoS）	DSCP（第 3 層）	補足
なし	（アクセス ルールにより定義された）このトラフィック等級に一致するパケットがイーグレス インターフェースから送出されるとき、802.1p タグは追加されません。	DSCP タグは明示的に 0 に設定（リセット）されます。	このトラフィック等級のターゲット インターフェースが VLAN 副インターフェースの場合、802.1q タグの802.1p 部分が明示的に 0 に設定されます。このトラフィック等級がVLAN 向けであり、優先順位付けに 802.1p が使用されている場合、「**維持**」、「**指定**」、「**参照**」方針を使用した特定のアクセス ルールをこのトラフィック等級に定義する必要があります。
維持	現存する 802.1p タグが維持されます。	現存する DSCP タグが維持されます。	
指定	表示されるドロップダウン メニューから明示的な 802.1p タグ値（0～7）を割り当てることができます。	表示されるドロップダウン メニューから明示的な DSCP タグ値（0～63）を割り当てることができます。	802.1p または DSCP 方針のどちらかを「**指定**」に設定し、もう一方を「**参照**」に設定した場合、明示的に指定された割り当てが最初に行われ、その後、もう一方がその割り当てに従って参照されます。
割付	「**オブジェクト > プロファイル オブジェクト > QoS 級割**」ページで定義された割付設定が、DSCP タグから802.1p タグへの割付に使用されます。	「**オブジェクト > プロファイル オブジェクト > QoS 級割**」ページで定義された割付設定が、802.1 タグからDSCP タグへの割付に使用されます。追加の「**802.1p 級割を、DSCP 値に優先する**」チェックボックスが表示されます。このチェックボックスを選択すると、割り付けられた 802.1p 値が、クライアントにより設定されたDSCP 値に優先して使用されます。これは、DSCP CoS 値を設定しているクライアントをオーバライドするのに有用です。	DSCP と 802.1p の両方で方針として「**参照**」を設定した場合、割付は一方向でのみ発生します。VLAN から 802.1p タグとともにパケットが到着した場合、DSCP が802.1p タグから割り付けられます。パケットが VLAN 宛ての場合、802.1p が DSCP タグから割り付けられます。

例として、下の画像では両方向の DSCP タグの方針を図示しています。

両方向 DSCP タグの方針



192.168.168.100 上のウェブ ブラウザから 10.50.165.2 上のウェブ サーバに対して HTTP アクセスを行うと、内部 (ペイロード) パケットと外部 (カプセル化 ESP) パケットに DSCP 値 8 のタグが付けられます。パケットがトンネルの反対側から出て、10.50.165.2 に配送されるとき、DSCP タグ値 8 が使用されます。10.50.165.2 からトンネル経由で応答パケットを (最初の SYN/ACKパケットから) 192.168.168.100 に送り返すとき、アクセス ルールにより、192.168.168.100 に配送される応答パケットに DSCP 値 8 のタグが付けられます。

この動作は、DSCP と 802.1p 級割の 4 つの QoS 方針設定のすべてに適用されます。

この動作の 1 つの実用的な応用例として、VPN ゾーン宛てのトラフィックに対する 802.1p 級割ルールの設定があります。VPN を横断して 802.1p タグを送信することはできませんが、VPN を横断して返された応答パケットに対して、トンネルからの出口で 802.1p タグを付けることができます。そのためには、物理的な送信インターフェースで 802.1p のタグ付けを有効にし、「[ゾーン] > VPNアクセス ルール」で「なし」以外の 802.1p 級割方式を設定する必要があります。

関連するネットワーク デバイスの 802.1p との互換性を確認し、該当する SonicWall インターフェース上で 802.1p 級割を有効にした後は、802.1p タグを管理するためにアクセス ルールの設定を開始できます。

下の表に示すように、**リモート サイト 1** ネットワークに対して 2 つのアクセス ルールを構成することができます。

リモート サイト 1: アクセス ルール設定の例

設定	アクセス ルール1	アクセス ルール2
「一般」ビュー		
動作	許可	許可
送信元ゾーン	LAN	VPN
送信先ゾーン	VPN	LAN
サービス	VoIP	VoIP
送信元	LAN プライマリ サブネット	メイン サイトのサブネット
送信先	メイン サイトのサブネット	LAN プライマリ サブネット
許可されたユーザ	すべて	すべて
スケジュール	常に有効	常に有効
Enable Logging (ログの有効化)	有効	有効

設定	アクセス ルール1	アクセス ルール2
断片化パケットを許可する	有効	有効
「Qos」ビュー		
DSCP 級割の方針	割付	割付
802.1p 級割を、DSCP 値に優先する	有効	有効
802.1p 級割の方針	割付	割付

最初のアクセス ルール（「**LAN > VPN**」を管理）は、以下の効果を持ちます。

- VPN 経由で **LAN プライマリ サブネット**から**メイン サイトのサブネット**に送信される、（サービス グループにより定義されている）**VoIP** トラフィックは、DSCP タグと 802.1p タグの両方に対して評価されます。
  - 「**割付**」に対する DSCP 級割方式と 802.1p 級割方式の組み合わせについては、「QoS 級割の管理」の表で説明しています。
  - 送信されたトラフィックに 802.1p タグ（例えば、CoS=6）のみが含まれている場合、VPN への内部（ペイロード）パケットは、DSCP 値 48 でタグ付けられます。また、外部（ESP）パケットも値 48 でタグ付けられます。
  - メイン サイトのファイアウォールによって戻りのトラフィックに DSCP タグ（CoS=48）が付けられていると仮定した場合、出口において CoS=6 の 802.1p タグが戻りのトラフィックに付けられます。
  - 送信されたトラフィックに DSCP タグ（例えば、CoS=48）のみが含まれている場合、DSCP 値が内部と外部の両方のパケットで維持されます。
  - メイン サイトのファイアウォールによって戻りのトラフィックに DSCP タグ（CoS=48）が付けられていると仮定した場合、出口において CoS=6 の 802.1p タグが戻りのトラフィックに付けられます。
  - 送信されたトラフィックに 802.1p タグ（CoS=6 など）と DSCP タグ（CoS=63 など）の両方が含まれている場合、802.1p タグが優先され、それに応じて割付が行われます。VPN への内部（ペイロード）パケットは、DSCP 値 48 でタグ付けられます。また、外部（ESP）パケットも値 48 でタグ付けられます。

メイン サイトのファイアウォールによって戻りのトラフィックに DSCP タグ（CoS=48）が付けられていると仮定した場合、出口において CoS=6 の 802.1p タグが戻りのトラフィックに付けられます。

2 番目のアクセス ルール（「VPN > LAN」）の効果を調べるには、メイン サイトで構成されたアクセス ルールを確認します（下を参照）。

メイン サイト: アクセス ルール設定の例

設定	アクセス ルール1	アクセス ルール2
「一般」ビュー		
動作	許可	許可
送信元ゾーン	LAN	VPN
送信先ゾーン	VPN	LAN
サービス	VoIP	VoIP
送信元	LAN サブネット	リモート サイト 1 サブネット
送信先	リモート サイト 1 サブネット	LAN サブネット
許可されたユーザ	すべて	すべて
スケジュール	常に有効	常に有効

設定	アクセス ルール1	アクセス ルール2
Enable Logging（ログの有効化）	有効	有効
断片化パケットを許可する	有効	有効
「Qos」ビュー		
DSCP 級割の方針	割付	割付
802.1p 級割を、DSCP 値に優先する	有効	有効
802.1p 級割の方針	割付	割付

VPN 経由で**リモート サイト 1 サブネット**からメイン サイトの LAN ゾーンの **LAN サブネット**に送信される、（サービス グループにより定義されている）**VoIP** トラフィックには、着信 VoIP 通話用のアクセス ルールが適用されます。VPN ゾーンに到着したトラフィックには、802.1p タグはなく、DSCP タグだけが付けられています。

- DSCP タグ（例えば CoS=48）を含んでいるトンネルを出て行くトラフィックでは、DSCP 値が維持されます。LAN 上の目的地へパケットが配送される前に、メイン サイトのファイアウォールによって、「**QoS 割付**」設定（例えば、CoS=6）に応じた 802.1p タグが付けられます。
- メイン サイトで電話を受けている VoIP 電話によって戻りのトラフィックに 802.1p タグ（例えば CoS=6）が付けられていると仮定した場合、戻りのトラフィックでは、VPN を経由して送り返される内部と外部の両方のパケットにおいて、変換割付に従って DSCP タグ（CoS=48）が付けられます。
- メイン サイトで電話を受けている VoIP 電話によって戻りのトラフィックに DSCP タグ（例えば CoS=48）が付けられていると仮定した場合、戻りのトラフィックでは、VPN を経由して送り返される内部と外部の両方のパケットにおいて、DSCP タグが維持されます。
- メイン サイトで電話を受けている VoIP 電話によって戻りのトラフィックに 802.1p タグ（例えば CoS = 6）と DSCP タグ（例えば CoS = 14）の両方が付けられていると仮定した場合、戻りのトラフィックでは、VPN を経由して送り返される内部と外部の両方のパケットにおいて、変換割付に従って DSCP タグ（CoS = 48）が付けられます。

用語集

- **802.1p** – IEEE 802.1p は、追加 16 ビットの 802.1q ヘッダー内で 3 プライオリティ ビット（合計 8 優先レベル）を使用することで、パケットにタグを付けるレイヤ 2（MAC レイヤ）CoS（サービス クラス）メカニズムです。802.1p 処理には、タグの生成、認識、処理を行うための互換性のあるデバイスが必要になり、互換性のあるネットワークでのみ採用する必要があります。
- **帯域幅管理（BWM）** – トラフィックのシェイピングやポリシングを行うために使用されるさまざまなアルゴリズムあるいは手法を指します。シェイピングは、送信トラフィックを管理することを表します。ポリシングとは、受信トラフィックを管理することを表します（受付制御とも呼ばれます）。帯域幅管理には、さまざまなキューイングおよび破棄手法を含め、それぞれ独自の設計上の長所を持つ多くの異なる方式があります。SonicWall では、特定のタイプの受信トラフィックに対する破棄手法に加え、受信および送信帯域幅管理用にトークン ベース、等級ベースのキューイング方式を採用しています。
- **Class of Service（CoS）** – レイヤ 2 またはレイヤ 3 のタグのように、分類後にトラフィックに適用される、指示子または識別子です。CoS 情報は、ネットワーク上のトラフィックの等級を区別するため、およびサービス品質（QoS）システム管理者によって定義された特殊な処理（例えば、優先キューイング、短い待ち時間など）を提供するために、QoS システムによって使用されます。
- **分類** – ある種別（等級）のトラフィックを識別（区別）する行為です。QoS のコンテキスト内では、遅延、待ち時間、またはパケット紛失に対するトラフィックの感度に基づいてカスタマイズされた処理（通常は優先す

るかどうか）を提供するために行われます。SonicOS では、アクセス ルールを使用して分類を行います。分類は、送信元ゾーン、送信先ゾーン、送信元アドレス オブジェクト、送信先アドレス オブジェクト、サービス オブジェクト、スケジュール オブジェクトのうちのいくつか、またはすべてに基づいて行うことができます。

- **コード ポイント** — ホストあるいは中間のネットワーク デバイスによって IP パケットの DSCP 部分にマーク付け（タグ付け）される値です。現在、タグ付けされたトラフィックの等級（昇順の優先順位）を定義するために、64（0～63）のコード ポイントを使用できます。
- **制限** — ネットワーク トラフィックにサービス品質を提供する多くの方法を記述するために使用される、広い意味を持つ用語です（破棄、キューイング、ポリシング、シェイピングを含みますが、これらに限定されるものではありません）。
- **DiffServ**（Differentiated Services）– 要件に基づいたトラフィックに合わせた処理を提供する目的で、IP ネットワーク上の異なるタイプや等級のトラフィックを区別するための基準です。DiffServでは、主に IP パケットの ToS ヘッダーの中でマークされたコード ポイント値に依存して、異なる等級のトラフィックを区別します。DiffServ のサービス レベルは、級割されたトラフィックが通過する各ルータ（または DiffServ が有効な他のネットワーク デバイス）上でホップ ベースで実行されます。現在、DiffServ のサービス レベルには、最低でも、既定、保証転送、緊急転送、および DiffServ があります。詳細については、「DSCP 級割」を参照してください。
- **破棄** — ネットワーク上で輻輳が発生するかもしれない時期の予測を試み、制限を超過したトラフィックを捨てることで輻輳を防ぐことを目的とする、QoS システムで採用されている輻輳回避メカニズムです。破棄は、キューがいっぱいになる状況を回避しようとするので、キューの管理アルゴリズムと見なすこともできます。高度な破棄メカニズムでは、取り扱いに慎重を要するトラフィックの破棄を回避するために CoS 級割が忠実に守られます。一般的な方式は、以下の通りです。
  - **テール ドロップ** — いっぱいになったキューを無差別に処理する方法で、パケットの CoS 級割にかかわらず、キューの中の最後のパケットが破棄されます。
  - **ランダム初期検知（RED）** — RED では、キューの状況を監視して、いついっぱいになるかを予測します。その後、グローバル同期の可能性を最小限にするために、ランダムにパケットを破棄します。RED の基本的な実装では、テール ドロップと同様に、CoS 級割は考慮されません。
  - **重み付けランダム初期検知（WRED）** — 破棄決定プロセスにおいて DSCP 級割を考慮する、RED の実装です。
- **DSCP**（Differentiated Services Code Points） — RFC2747 に規定されている IP ヘッダーの ToS フィールドの再利用です。DSCP では、64 のコード ポイント値を使用して、DiffServ（Differentiated Services）を有効にします。その等級によってトラフィックを級割することによって、各パケットをネットワークに沿ったすべてのホップで適切に処理することができます。
- **グローバル同期** — キューがいっぱいになることに対処するために設計された輻輳回避方法である破棄の潜在的な副作用です。グローバル同期は、輻輳したリンクを通過する複数の TCP フローが同時に破棄されたとき（例えばテール ドロップ）に発生します。これらのフローのそれぞれに対して、ネイティブな TCP スロースタート メカニズムがほぼ同時に開始されると、リンクはこれらのフローによって再び溢れてしまいます。その結果、輻輳と不十分な利用が周期的に発生します。
- **保証帯域幅** — ある等級のトラフィックに常に与えられる、インターフェース上で利用可能な合計帯域幅に対して宣言された割合です。受信 BWM と送信 BWM の両方に適用されます。すべての BWM ルールにおける保証された帯域幅の合計は、利用可能な帯域幅の合計の 100%を超過することはできません。SonicOS では帯域幅管理機能が拡張され、速度制限機能を使用できます。第 2 層、3層、または 4 層ネットワーク トラフィックの最大速度を指定するトラフィック ポリシーを作成できます。これにより、プライマリ WAN リンクから、あまり多数のトラフィックを処理できないバックアップ接続へのフェイルオーバーが生じた場合でも、帯域幅管理が行えます。「保証された帯域幅」は 0%に設定することもできます。
- **受信（イングレスまたは IBWM）** — 特定のインターフェースに入るトラフィックの速度のシェイピングを行う機能です。TCP トラフィックに対しては、送信の承認（ACK）を遅らせ、送信元での速度を遅くさせることで、受

信フローの速度を調整可能にして、実際のシェイピングを行うことができます。UDP トラフィックの場合、UDP にはネイティブなフィードバック制御がないので、破棄手法が使用されます。

- **IntServ** — RFC1633 で定義された統合サービス (Integrated Services) です。DiffServ のバックアップCoS システムである IntServ は、各機器がトラフィックを送信する前にネットワーク要件を要求 (または予約) する点で、DiffServ と根本的に異なります。これには、ネットワーク上の各ホップが IntServ 対応である必要があり、また、各ホップですべてのフローの状態情報を保持する必要があります。SonicOS では、IntServ はサポートされません。IntServ の最も一般的な実装は RSVP です。
- **最大帯域幅** — ある等級のトラフィックに許可される最大帯域幅を定義する、インターフェース上で利用可能な合計帯域幅に対して宣言された割合です。受信 BWM と送信 BWM の両方に適用されます。帯域幅の速度制限を指定する調整メカニズムとして使用されます。帯域幅管理機能が拡張され、速度制限機能が使用できます。第 2 層、3層、または 4 層ネットワークトラフィックの最大速度を指定するトラフィック ポリシーを作成できます。これにより、プライマリ WANリンクが大量のトラフィックを処理できないバックアップ接続にフェイルオーバーする場合の帯域幅管理が可能になります。「最大帯域幅」は 0%に設定することもできます。その場合、すべてのトラフィックが遮断されます。
- **送信 (イーグレスまたは OBWM)** — インターフェースからトラフィックを送出する速度を制限することです。送信BWM では、8 つの優先順位キューを持つクレジット (またはトークン) ベースのキューイング システムを使用して、アクセス ルールによって分類される異なるタイプのトラフィックを処理します。
- **優先順位** — トラフィックの分類で使用される追加要素です。SonicOS では、8 つの優先順位リング (0 = 最高、7 = 最低) を使用して、帯域幅管理に使用されるキュー構造を構成しています。キューは、優先順位リングの順序で処理されます。
- **割付** – SonicOS による QoS の実装に関していえば、割付は、802.1p タグ付けをサポートしないネットワーク リンクを横断する 802.1p のタグを保持するために、レイヤ 2 CoS タグ (802.1p) とレイヤ 3 CoS タグ (DSCP) を相互に変換する機能です。割付の対応付けは、完全にユーザ定義可能で、また、割付の動作はアクセス ルールによって制御されます。
- **級割 (タグ付けまたは色付けとも呼ばれます)** — 区別の目的でレイヤ 2 (802.1p) またはレイヤ 3 (DSCP) の情報をパケットに適用する行為です。その結果、パケットは、宛先へのパス上にあるネットワーク デバイスにより、適切に分類 (認識) され、優先順位が付けられます。
- **マルチ プロトコル ラベル スイッチング (MPLS)** – この用語は QoS の分野でよく使用されますが、(SonicWall 装置を含む) ほとんどの顧客構内 IP ネットワーク デバイスでネイティブにサポートされません。MPLS は、ネットワークに沿って概念的な接続志向のパス (LSP:ラベル スイッチ パス) を追加することにより IP ネットワーク機能を強化する、キャリア クラスのネットワーク サービスです。パケットが顧客構内ネットワークから外に出るときに、パケットはラベル エッジ ルータ (LER) によってタグ付けされます。これにより、ラベルを使用して LSP を判定できるようになります。MPLS タグ自体は第 2 層と第 3 層の間に存在し、両方のネットワークの層の MPLS 特性を伝えます。MPLS は、第 2 層と第 3 層の VPN サービスの両方を提供する一方、既存の IPSec VPN 実装との相互運用が可能であるため、VPN で一般的になりつつあります。また、MPLS は、QoS 能力についても非常によく知られており、従来の DSCP 級割とも相互運用が可能です。
- **ホップ単位動作 (PHB)** — パケットが通過する各 DiffServ 対応ルータにおいて、パケットの DSCP 分類に基づいてパケットに適用される処理。破棄、再級割 (再分類)、最大努力型、保証転送、緊急転送などの動作があります。
- **ポリシング** — ネットワーク リンクを出入りするトラフィックの速度を制御する、トラフィックの制限機能。ポリシングの方法は、無差別にパケットを捨てる方式からアルゴリズムによるシェイピングまで、またさまざまなキューイング規則まで及びます。

- **キューイング** — リンクの利用可能な帯域幅を効果的に使用できるように、トラフィックを分類した後に、並べ替えのため、および個別に管理するために、キューが一般的に使われます。キューは、高優先順位のキューが常に多くのトラフィックを受信でき、低優先順位のキューよりも優先してサービスを受ける（キューからパケットが取り出される、または処理される）ように、さまざまな方式とアルゴリズムを使用して管理されます。以下に、いくつかの一般的なキュー規則を示します。
  - **FIFO (First In First Out、先入れ先出し)** – 最初に入ったパケットが最初に処理される、非常に単純な無差別型のキュー。
  - **等級ベース キューイング (CBQ)** — 高優先順位のトラフィックが優先的に処理される、パケットの CoS を考慮に入れたキューイング規則。
  - **重み付け公平キューイング (WFQ)** — パケットの IP 優先順位とフローの合計数に基づいた単純な式を使用してキューをサービスする規則。WFQ は、サービスを受ける高優先順位のフローが異常に大量にあると不安定になる傾向があり、望みとは逆の効果が生じることがしばしばあります。
  - **トークン ベース CBQ** — トークンを使用した CBQ の拡張。または、リンクの利用を円滑化または正常化して、過剰利用や不十分な利用を回避するのに役立つクレジット ベースのシステム。SonicOS の帯域幅管理で採用されています。
- **リソース予約プロトコル (RSVP)** – 一部のアプリケーションで採用されている IntServ シグナリング プロトコルであり、ネットワーク動作（例えば、遅延や帯域幅）をネットワーク パスに沿って予約できるように、ネットワーク動作の事前要求が行われます。この予約パスを設定するには、パスに沿った各ホップが RSVP に対応しており、それぞれが要求されたリソースを予約することに同意する必要があります。この QoS システムは、現存しているフローの状態を各ホップが維持することを要求するため、いくぶんリソース集約的です。IntServの RSVP は DiffServ の DSCP とはかなり異なりますが、相互運用することができます。SonicOS では、RSVP はサポートされません。
- **シェイピング** — 通常、送信元に対する何らかのフィードバック メカニズムを用意することによってトラフィック フローの速度を変更するための、QoS システムによる試み。これの最も一般的な例は、TCP 速度の操作です。つまり、TCP 送信元に送り返す承認（ACK）をキューに入れることによって遅延させ、算出されるラウンドトリップ時間（RTT）を増加させます。これにより、TCP 固有の動作を利用して、送信元がデータを送信する速度を低下させます。
- **サービス種別 (ToS)** — CoS 情報を指定することのできる、IP ヘッダー内部のフィールド。歴史的にごくまれに、IP 優先順位ビットとともに、CoS を定義するために使用されていました。現在、ToS フィールドは、DiffServ のコード ポイント値により、一般的に使用されています。

4

コンテンツ フィルタ

SonicWall コンテンツ フィルタ サービス (CFS) バージョン 4.0 では、教育機関、企業、図書館、政府機関向けにコンテンツ フィルタが強化されています。こうした組織では、コンテンツ フィルタ オブジェクトの活用により、ウェブサイトを制御したり、学生や従業員が IT 部門から支給されたコンピュータを使用して組織のファイアウォールの背後からのアクセスを行ったりできるようになります。

ⓘ **補足:** 古いバージョンから CFS 4.0 へのアップグレードについては、『*SonicWall コンテンツ フィルタ サービス アップグレード ガイド*』を参照してください。また、これらのオブジェクトを CFS ポリシーに適用するには、「*SonicOS セキュリティ設定*」技術文書の「*ポリシー > ルールとポリシー > コンテンツ フィルタ ルール*」セクションを参照してください。

トピック:

CFS プロファイル オブジェクトの管理

トピック:

CFS プロファイル オブジェクトについて

CFS プロファイル オブジェクトは、各 HTTP/HTTPS 接続に対してトリガされる動作を定義します。

名前	CFS プロファイル オブジェクトの名前。既定の名前は **CFS Default Profile** です。既定のオブジェクトは編集可能ですが、削除はできません。
許可 URI リスト	許可リストに記載された URI リスト オブジェクトの名前。
禁止 URI リスト	禁止リストに記載された URI リスト オブジェクトの名前。
遮断種別	CFS プロファイル オブジェクトによって遮断されるすべての種別の名前。
パスワード種別	CFS プロファイル オブジェクトによってパスワードが要求されるすべての種別の名前。
確認種別	CFS プロファイル オブジェクトによって確認が要求されるすべての種別の名前。
帯域幅管理種別	この CFS プロファイル オブジェクトによって制御される帯域幅管理のすべての種別の名前。
許可種別	CFS プロファイル オブジェクトによって許可されるすべての種別の名前。
コメント	CFS プロファイル オブジェクトの作成中に追加されたコメント
UUID	UUID (Universally Unique Identifier) は、36 文字の文字列 (32 文字の英数字と 4 つのハイフン) です。SonicWall ネットワーク セキュリティ装置上でプロファイル オブジェクト/グループなどのエンティティを一意に識別するために使用されます。SonicOS UUID は、システムによって生成される読み取り専用の内部値です。

CFS プロファイル オブジェクト 用 UUID について

SonicOS 6.5.3 (以降) は、コンテンツ フィルタ オブジェクトの UUID (Universally Unique Identifier) を自動的に生成してバインドします。

UUID は、ハイフンで区切られた 5 文字のグループで表示された 32 桁の 16 進数で構成されています。UUID は、オブジェクトの作成時に生成されます。そのオブジェクトを変更したり、ファイアウォールを再起動しても変化しません。UUID は、オブジェクトが削除されると削除され、削除された UUID は再利用されません。UUID は、装置を工場出荷時の既定の設定で再起動すると再生成されます。

CFS プロファイル オブジェクトの設定

既定の CFS プロファイル オブジェクトである **CFS Default Profile** は、SonicOS によって作成されます。この CFS プロファイル オブジェクトは、構成および編集は可能ですが、削除することはできません。

CFS プロファイル オブジェクトを構成するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」ページに移動します。
2. ページの上部にある「**追加**」ボタンを選択します。「**CFS プロファイル オブジェクトの追加**」ダイアログが表示されます。

3. 「**設定**」画面で、「**名前**」フィールドに CFS プロファイル オブジェクトの名前を入力します。
4. 「**許可 URI リスト**」ドロップダウン メニューから、無制限のアクセスを許可する URI が記載された URI リスト オブジェクトを選択し、このリストをホワイト リストとして扱います。
   - 「なし」(既定)
   - URI リスト オブジェクトの名前。
   - 「URI リスト オブジェクトの作成」。このオプションを選択すると、「CFS URI リスト オブジェクトの追加」ダイアログが表示されます。URI リスト オブジェクトを作成する方法については、SonicOS の「*オブジェクト > 一致オブジェクト > URI リスト*」セクションを参照してください。
5. 「**禁止 URI リスト**」ドロップダウン メニューから、アクセスを一切認めない URI が記載された URI リスト オブジェクトを選択し、このリストをブラック リストとして扱います。
   - 「なし」(既定)
   - URI リスト オブジェクトの名前。
   - 「URI リスト オブジェクトの作成」。このオプションを選択すると、「CFS URI リスト オブジェクトの追加」ダイアログが表示されます。URI リスト オブジェクトを作成する方法については、SonicOS の「*オブジェクト > 一致オブジェクト > URI リスト*」セクションを参照してください。
6. 「**URI リストの検索順序**」ドロップダウン メニューから、フィルタリング中に最初に検索される URI リストを選

択します。

- 「許可 URI リストを優先」(既定)
- 禁止 URI リストを優先

7. 「**禁止 URI リストに対する操作**」ドロップダウン メニューから、禁止リストにある URI が出現した場合に実行する動作を選択します。

遮断 (既定)	CFS 動作オブジェクト用に構成された遮断ページが、サイトにアクセスしようとしたユーザに表示されます。
確認	CFS 動作オブジェクト用に構成された確認ページが、サイトにアクセスしようとしたユーザに表示されます。ユーザにはアクセスの意思確認が求められます。
パスワード	CFS 動作オブジェクト用に構成されたパスワード ページが、サイトにアクセスしようとしたユーザに表示されます。ユーザは、サイトに入るために有効なパスワードを入力する必要があります。

8. 「**種別構成**」セクションには、芸術/エンターテイメント、ビジネス、教育、旅行、武器、ショッピングなど、すべての URI 種別が記載されています。種別ごとの動作ではなく、すべての URI に共通して実行される動作を構成できます。リストを下へスクロールしながら、各種別のドロップダウン メニューから動作を選択します。

   - 許可
   - 遮断
   - 帯域幅管理
   - 確認
   - パスワード

   ⓘ | **補足:** 既定では、種別 1 ～ 12 および種別 59 が遮断され、残りの種別は許可されています。

   - すべての種別を同じ動作に変更するには、以下の手順に従います:
     1. 「**操作**」ドロップダウン メニューから動作を選択します。
     2. 「**すべてに設定**」ボタンをクリックします。
   - すべての種別を既定の動作にリセットするには、「**既定**」ボタンを選択します。
9. スマート フィルタとセーフ サーチのオプションを有効にするには、「**詳細**」タブを選択します。この画面でオプションを設定する方法については、「詳細画面」を参照してください。
10. ウェブの時限閲覧に関する規約を設定するには、「**時限閲覧規約**」タブを選択します。この画面でオプションを設定する方法については、「規約画面」を参照してください。
11. ユーザ定義ヘッダー挿入を構成するには、「**ユーザ定義ヘッダー**」タブをクリックします。この画面でオプションを設定する方法については、「ユーザ定義ヘッダー画面」を参照してください。
12. 「**追加**」を選択します。「**CFS プロファイル オブジェクト**」テーブルが更新されます。

トピック:

- 詳細画面
- 規約画面
- ユーザ定義ヘッダー画面

詳細画面

この画面は、「**CFS プロファイル オブジェクトの追加**」ダイアログの 4 つの画面の 1 つです。ダイアログを開くには、「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。次に「**詳細**」タブをクリックします。

ⓘ | **補足:** 既定では、すべてのオプションがオフになっています。

1. HTTPS サイトに対してコンテンツ フィルタを有効にするには、「**HTTPS コンテンツ フィルタを有効にする**」オプションを選択します。このポリシーベースの HTTPS コンテンツ フィルタ オプションは、SonicOS 6.5.3 以降で使用できます。これは、「**ポリシー > セキュリティ サービス > コンテンツ フィルタ**」ページ上の以前のバージョンのグローバル HTTPS コンテンツ フィルタ オプションの代わりに使われます。

   ⓘ | **補足:** DPI-SSL クライアント検査が有効で、検査のためにコンテンツ フィルタが選択されている場合は、その検査が優先され、ポリシーベースの HTTPS コンテンツ フィルタ設定は無視されます。具体的には、「**ポリシー > DPI-SSL**」ページの「**SSL クライアント検査を有効にする**」および「**コンテンツ フィルタ**」オプションを有効にすると、CFS ポリシーの「**HTTPS コンテンツ フィルタを有効にする**」オプションは無視されます。この場合、DPI-SSL は接続を復号化し、後でフィルタリングのためにプレーン テキストとして CFS に送信します。

   HTTPS コンテンツ フィルタは IP ベースであり、URL を検査しませんが、他の方法を使用して URL 格付けを取得します。このオプションを有効にすると、CFS は URL 格付け検索を次の順序で実行します。

   a. クライアント *hello* を検索してサーバ名を探します。CFS は、サーバ名を URL 格付けの取得に使用します。
   b. サーバ名が使用できない場合は、SSL 証明書を検索してコモンネームを探します。CFS は、コモンネームを URL 格付けの取得に使用します。
   c. サーバ名もコモンネームも使用できない場合は、CFS は、IP アドレスを URL 格付けの取得に使用します。

   HTTP コンテンツ フィルタで認証の強制のためにリダイレクトまたは遮断ページの提供を実行できますが、HTTPS フィルタでページの遮断はユーザに対し通知されることなく行われます。

2. Google 翻訳 (*https://translate.google.com*) 内の埋め込み URL を検出し、埋め込み URI をフィルタリングするには、「**埋め込み URI に対してスマート フィルタを有効にする**」オプションをオンにします。

   ⓘ | **重要:** この機能が動作するには、クライアント DPI-SSL のコンテンツ フィルタが有効化されている必要があります。

   ⓘ | **補足:** この機能は、Google にのみ適用されます。対象となるのは、現在レーティングが済んでいる埋め込みウェブサイトです。

3. 以下のウェブサイトのいずれかで検索するときにセーフ サーチを適用するには、「**セーフ サーチ強制を有効にする**」オプションをオンにします。

    - *www.yahoo.com*
    - *www.ask.com*
    - *www.dogpile.com*
    - *www.lycos.com*

    ⓘ **補足:** この強制は、ポリシー レベルでは構成できません。この機能では、HTTPS サイトへの DNS リダイレクションが使用されるためです。HTTPS サイトについては、クライアント DPI-SSL コンテンツ フィルタが有効化されている必要があります。
4. 脅威 API を有効にするには、「**脅威 API 強制を有効にする**」オプションをオンにします。

    ⓘ **補足:** SonicOS が最初の脅威リストを受信したときに作成する脅威 URI リスト オブジェクトは、「**脅威 API 強制を有効にする**」をオンにすることで参照されます。
5. Google 用のセーフ サーチ オプションを各 CFS ポリシーとそれに対応する CFS 動作に優先して適用するには、「「**Google セーフ サーチ強制」を有効にする**」オプションを選択します。

    ⓘ **補足:** 通常、セーフ サーチは自動的に適用され、Google によって管理されますが、このオプションをオンにすると、SonicOS は DNS 応答の中の Google ドメインを、Google セーフ サーチ仮想 IP アドレスに書き換えます。

    ⓘ **補足:** この機能は、クライアント ホストの DNS キャッシュが更新されるまで反映されません。
6. YouTube に制限付きモード (セーフ サーチ) でアクセスするには、「**YouTube 制限付きモードを有効にする**」オプションを選択します。

    ⓘ **補足:** YouTube では、ユーザやその他の警告によって報告された不適切なコンテンツを含む可能性のある動画を除外する新機能が提供されています。この機能が有効化されていると、SonicOS は YouTube ドメインの DNS 応答をセーフ サーチ仮想 IP アドレスに書き換えます。

    ⓘ **補足:** この機能は、クライアント ホストの DNS キャッシュが更新されるまで反映されません。
7. Bing 用のセーフ サーチ オプションを各 CFS ポリシーとそれに対応する CFS 動作に優先して適用するには、「「**Bing セーフ サーチ強制」を有効にする**」オプションを選択します。

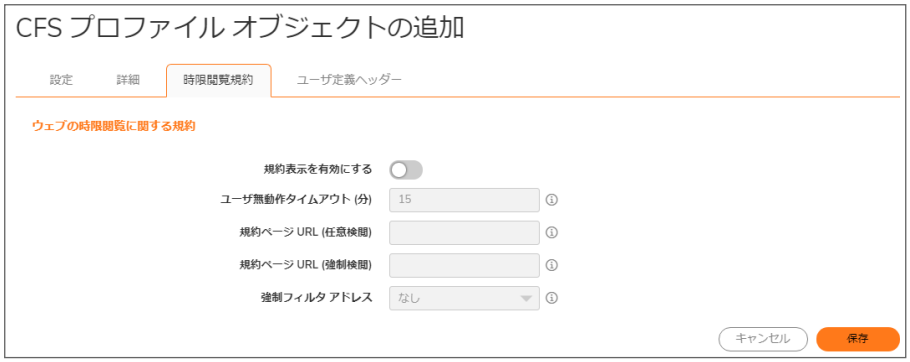
    ⓘ **補足:** この機能が有効化されていると、SonicOS は Bing ドメインの DNS 応答をセーフ サーチ仮想 IP アドレスに書き換えます。

    ⓘ **補足:** この機能は、クライアント ホストの DNS キャッシュが更新されるまで反映されません。
8. 「**保存**」をクリックします。

規約画面

この画面は、「**CFS プロファイル オブジェクトの追加**」ダイアログの 4 つの画面の 1 つです。ダイアログを開くには、「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。次に、「**時限閲覧規約**」タブをクリックします。

ⓘ **補足:** 時限閲覧規約は、HTTP 要求に対してのみ機能します。HTTPS 要求は、「確認」(同意) ページにはリダイレクトできません。



1. ユーザがアクセス前に同意が必要なサイトを訪れたときに「時限閲覧規約」(確認) ページを表示するには、「**規約表示を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。このオプションを選択すると、他のオプションが使用できるようになります。
2. 「時限閲覧規約」ページが表示される時間の期限をユーザに通知するには、無動作時間の長さを「**ユーザ無動作タイムアウト (分)**」フィールドに入力します。無動作時間の最小値は 1 分、最大値は 9999 分、既定値は 15 分です。
3. 規約への同意が必要なウェブサイトにユーザが移動したときにそのユーザをリダイレクトするウェブサイトの URL を「**規約ページURL (任意検閲)**」フィールドに入力します。「時限閲覧規約」ページは、次の条件を満たす必要があります。
    - ウェブ サーバ上に存在し、ネットワーク上でユーザが URI を通じてアクセス可能。
    - SonicWall 装置内の以下の 2 つのページへのリンクが含まれる。このリンクを選択すると、ユーザが希望するアクセスの種別がファイアウォールに通知されます。
        - フィルタなしのアクセス: *<appliance's LAN IP address>/iAccept.html*
        - フィルタありのアクセス: *<appliance's LAN IP address>/iAcceptFilter.html*
4. 強制的な検閲を要求するウェブサイトにユーザが移動したときにそのユーザをリダイレクトするウェブサイトの URL を「**規約ページURL (強制検閲)**」フィールドに入力します。「時限閲覧規約」ページは、次の条件を満たす必要があります。
    - ウェブ サーバ上に存在し、ネットワーク上でユーザが URI を通じてアクセス可能。
    - SonicWall 装置内の「*<appliance's LAN IP address>/iAcceptFilter.html*」ページへのリンクが含まれる。これは、ユーザが閲覧の検閲を承諾することをファイアウォールに通知します。
5. 「**強制フィルタ アドレス**」ドロップダウン メニューから、強制的な検閲を要求する構成済み IP アドレスが含まれるアドレス オブジェクトを選択します。
6. 「**保存**」をクリックします。

ユーザ定義ヘッダー画面

SonicOS 6.5.1 以降では、ファイアウォールをウェブ プロキシ サーバとして構成できます。これにより、提供したアカウントとは異なるアカウントでユーザがウェブ サービスにサインインできないようにする、またはユーザが閲覧できるコンテンツを制限するなど、ウェブ サービスの制御を行えます。ウェブ プロキシ サーバは、コンテンツ フィルタ ポリシーに一致するすべてのトラフィックにユーザ定義ヘッダーを追加します。このヘッダーによって、ウェブ サービスにアクセスできるユーザのドメイン、またはユーザがアクセス可能なコンテンツが識別されます。DPI-SSL が有効の場合、暗号化された HTTPS トラフィックがサポートされます。

この画面は、「**CFS プロファイル オブジェクトの追加**」ダイアログの 4 つの画面の 1 つです。ダイアログを開くには、「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」ページに移動して、ページ上部の「**追加**」ボタンをクリックします。次に、「**ユーザ定義ヘッダー画面**」タブをクリックします。

この機能には次の設定が必要です。

- コンテンツ フィルタ サービスが有効になっている。
- 一致する CFS プロファイル オブジェクトで、ユーザ定義ヘッダーの挿入が有効になっている。
- ユーザ定義ヘッダーを挿入する暗号化された HTTPS 要求に対して、DPI-SSL が有効になっている。

CFS ユーザ定義ヘッダーを構成し、ユーザ定義ヘッダー挿入を有効にするには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」タブに移動します。
2. ページの上部にある「**追加**」を選択します。
3. 「**CFS プロファイル オブジェクトの追加と編集**」ダイアログで、「**ユーザ定義ヘッダー**」タブをクリックし、「ユーザ定義ヘッダー挿入」オプションを表示します。
4. 「**ユーザ定義ヘッダー挿入を有効にする**」オプションを有効にします。
5. **追加**アイコンをクリックし、ユーザ定義ヘッダー エントリの「**ドメイン**」、「**鍵**」、「**値**」を構成します。

「**ドメイン**」は、HTTP 要求内のホストがエントリに一致するかどうかをパケットの処理中に確認するために使用されます。「**キー**」と「**値**」は、ユーザ定義ヘッダー挿入の実行時データが作成される際に、エントリに対する適切なヘッダーを生成するために必要です。

「ドメイン」の命名規則は次のとおりです。

- ドメイン名は、最大 16 のトークンを含むことができます。トークンは、ピリオド (.) で区切ります。
- ドメイン名の先頭と末尾には、区切り文字を使用できません。
- 各トークンは、最大で 128 文字の印刷可能な ASCII 文字を含むことができます。
- ドメイン名のトークンに使用できる文字は、*0-9a-zA-z$-_+!'(),* のみです。
- IPv4/IPv6 のアドレスを、"[2001:2002:2003::2005:2006]" のように、ドメイン名として定義できます。

6. 「**保存**」をクリックします。

CFS プロファイル オブジェクトの編集

CFS プロファイル オブジェクトを編集するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」ページに移動します。
2. 編集する CFS プロファイル オブジェクトにマウス カーソルを重ね、**編集**アイコンをクリックします。「**CFS プロファイル オブジェクトの編集**」ダイアログが表示されます。このダイアログは、「**CFS プロファイル オブジェクトの追加**」ダイアログと同じです。
3. 変更を行うには、「CFS プロファイル オブジェクトの設定」の適切な手順に従ってください。

CFS プロファイル オブジェクトの削除

CFS プロファイル オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > コンテンツ フィルタ**」ページに移動します。
2. 以下のいずれかを実行します。
   - 削除するプロファイル オブジェクトにマウス カーソルを重ね、**削除**アイコンをクリックします。
   - 削除する 1 つ以上のプロファイル オブジェクトのチェックボックスをクリックし、ページ上部の**削除**アイコンをクリックします。

コンテンツ フィルタ オブジェクトの適用

コンテンツ フィルタ オブジェクトの設定が終わった後で、オブジェクトをコンテンツ フィルタ ポリシーに適用する必要があります。コンテンツ フィルタの設定は、「**ポリシー セキュリティ サービス > コンテンツ フィルタ**」ページで行えます（『*SonicOS セキュリティ設定*』技術文書の「*コンテンツ フィルタリング サービスの設定*」セクションを参照）。

5

DHCP オプション

SonicWall ネットワーク セキュリティ装置には、IP アドレス、サブネット マスク、ゲートウェイ アドレス、および DNS サーバ アドレスをネットワーク クライアントに配布する DHCP (Dynamic Host Configuration Protocol) サーバが搭載されています。「**ネットワーク > DHCP サーバ**」には、装置の DHCP サーバ、リース スコープ、DHCP リースの設定が含まれます。

SonicWall DHCP サーバ オプション機能は、主に RFC 2131 および 2132 で定義される、ベンダー拡張とも呼ばれる DHCP オプションのサポートを提供します。これらのオプションは、主に RFC 2131 および RFC 2132 で定義されている機能です。DHCP オプションを使用すると、あらかじめ定義されたベンダー固有の情報を追加的なDHCP パラメータとして指定することができ、指定した情報は DHCP メッセージのオプション フィールドに格納されます。そのため、DHCP メッセージの送信により、ネットワーク上のクライアントに対してベンダー固有の設定情報およびサービス情報を提供することができます。RFC で定義された DHCP オプション番号に関する詳細は、以下を参照してください。

- IPv4 オプション: RFC で定義された DHCPV4 オプション番号
- IPv6 オプション: RFC で定義された DHCPV6 オプション番号

DHCP オプション オブジェクトの設定

次のいずれかの方法で DHCP オプション オブジェクトを作成できます。

1. 「**オブジェクト > プロファイル オブジェクト > DHCP オプション**」ページに移動し、「**追加**」をクリックして IPv4 および IPv6 DHCP オプション オブジェクトを作成します。「DHCP オプション オブジェクトの追加」ダイアログが表示されます。

2. 「**オプション名**」フィールドにオプション オブジェクトの名前を入力します。

3. 「**オプション番号**」で、目的の DHCP オプションに対応するオプション番号を選択します。オプションの番号、名前、および説明の一覧については、以下を参照してください。
    - IPv4 については、「RFC で定義された DHCPV4 オプション番号」を参照してください
    - IPv6 については、「RFC で定義された DHCPV6 オプション番号」を参照してください
4. 次の場合:
    - 「**オプション番号 2 (タイム オフセット)**」を選択したときなど、該当するオプション種別が 1 つしかない場合、「**オプション配列**」は淡色表示されます。**ステップ 7** に進みます。
    - 例えば、「**77 (ユーザ クラス情報)**」では、「**オプション種別**」が使用可能になり、このオプションで使用できるタイプとして「**IP アドレス**」、「**2 バイト データ**」、「**文字列**」、「**論理型**」などがリストされます。オプション種別を選択します。
5. オプションの値 (例えば、IP アドレスなど) を「**オプション値**」フィールドに入力します。「オプション配列」チェックボックスがオンの場合は、複数の値をセミコロン (;) で区切って入力することができます。
6. 「**OK**」をクリックします。設定したオブジェクトが「**オプション オブジェクト**」テーブルに表示されます。

DHCPV4 の「オプション オブジェクト」テーブル

DHCPV6 の「オプション オブジェクト」テーブル

または

- 「**ネットワーク > DHCP サーバ > DHCP サーバ リース 範囲**」タブに移動し、
    - IPv4 オプション オブジェクトを作成するには、「**静的登録の追加**」または「**動的登録の追加**」オプションをクリックします。ダイアログで、「**詳細**」タブをクリックして「**DHCP 汎用オプション グループ**」ドロップダウンから「**DHCP オプション オブジェクトの作成**」を選択します。

- IPv6 オプション オブジェクトを作成するには、「**IPv6**」タブを選択して「**静的登録の追加**」または「**動的登録の追加**」オプションをクリックします。ダイアログで、「**詳細**」タブをクリックして「**DHCP 汎用オプション**」ドロップダウンから「**DHCP オプション オブジェクトの作成**」を選択します。

- 上のセクションのステップ 2 からステップ 6 に従ってください。設定したオブジェクトが「**オプション オブジェクト**」テーブルに表示されます。

RFC で定義された DHCPV4 オプション番号

オプション番号	名前	説明
2	タイム オフセット	協定世界時からのオフセット時間
3	ルータ	N/4 ルータのアドレス
4	タイム サーバ	N/4 タイム サーバのアドレス
5	ネーム サーバ	N/4 IEN-116 ネーム サーバのアドレス
6	DNS サーバ	N/4 DNS サーバのアドレス
7	ログ サーバ	N/4 ログ サーバのアドレス
8	Cookie サーバ	N/4 Cookie サーバのアドレス
9	LPR サーバ	N/4 プリンタ サーバのアドレス
10	Impress サーバ	N/4 Imagen Impress サーバのアドレス
11	RLP サーバ	N/4 リソース ロケーション サーバのアドレス
12	ホスト名	ホスト名の文字列 ((サーバ ユニキャスト) など)
13	ブートファイル サイズ	ブート ファイルのサイズ (512 バイト ブロックの数)
14	メリット ダンプ ファイル	クライアントのコア イメージがダンプされるファイルの名前
15	ドメイン名	クライアントの DNS ドメイン名
16	Swap サーバ	スワップ サーバのアドレス
17	ルート パス	ルート ディスクのパス名
18	拡張ファイル	追加的な BOOTP 情報が含まれているパッチ名
19	IP レイヤ転送	IP 転送の有効化または無効化
20	ソース ルーティング有効	ソースルーティングの有効化/無効化
21	ポリシー フィルタ	ルーティングに対するポリシー フィルタ

オプション番号	名前	説明
22	最大 DG 再編成 サイズ	再組み立てを行うデータグラムの最大サイズ
23	既定の IP TTL	既定の IP 存続期間
24	パス MTU 寿命 タイムアウト	パス MTU のエージングに適用するタイムアウト時間
25	MTU 停滞	パス MTU 検出の実行時に使用する MTU サイズのテーブル
26	インターフェース MTU サイズ	インターフェース MTU サイズ
27	すべてのサブネットはローカル	すべてのサブネットにローカルの MTU を適用可能か否かを指定
28	ブロードキャスト アドレス	ブロードキャスト アドレス
29	マスク検出の実行	マスク検出を実行するか否かを指定
30	マスクを他者に提供	サブネット マスク要求に応答するか否かを指定
31	ルータ検出の実行	ルータ検出を実行するか否かを指定
32	ルータ要請アドレス	ルータ要請メッセージの送信先アドレス
33	静的ルーティング テーブル	静的ルーティング テーブル
34	Trailer カプセル化	トレーラの使用を試みるか否かを指定
35	ARP キャッシュ タイムアウト	ARP キャッシュのタイムアウト時間
36	イーサネット カプセル化	イーサネットのカプセル化を使用するか否かを指定
37	既定の TCP 持続時間	既定の TCP 持続時間
38	TCP キープアライブ間隔	TCP キープアライブ メッセージの送信間隔
39	TCP キープアライブ ガーベイジ	TCP キープアライブ メッセージとともに互換性のための無意味なバイトを送信するか否かを指定
40	NIS ドメイン名	NIS ドメイン名
41	NIS サーバ アドレス	NIS サーバ アドレス
42	NTP サーバ アドレス	NTP サーバ アドレス
43	ベンダー固有情報	ベンダー固有情報
44	NetBIOS ネーム サーバ	NetBIOS ネーム サーバのアドレス
45	NetBIOS データグラム ディストリビューション	NetBIOS データグラム ディストリビューションサーバのアドレス
46	NetBIOS ノード種別	NetBIOS ノードの種類
47	NetBIOS スコープ	NetBIOS スコープ
48	X Window フォント サーバ	X Window フォント サーバのアドレス
49	X ウィンドウディスプレイマネージャ	X ウィンドウディスプレイマネージャが実行されているシステムのアドレス
50	要求された IP アドレス	要求された IP アドレス

オプション番号	名前	説明
51	IP Address Lease Time	IP アドレスのリース期間
52	Option Overload	“sname”または“file”フィールドをオプション用に使用していることを示す
53	DHCP Message Type	DHCP メッセージの種類
54	DHCP サーバ証明	DHCP サーバの識別情報
55	Parameter Request List	要求するパラメータのリスト
56	メッセージ	DHCP エラー メッセージ
57	DHCP Maximum Message Size	DHCP メッセージの最大サイズ
58	Renew Time Value	DHCP リースの再取得を要求するまでの時間 (T1)
59	Rebinding Time Value	DHCP 再割り当てを要求するまでの時間 (T2)
60	クラス識別子	クラス識別子
61	クライアント識別子	クライアント識別子
62	Netware/IP ドメイン名	Netware/IP ドメイン名
63	Netware/IP サブ オプション	Netware/IP サブ オプション
64	NIS+ V3 クライアント ドメイン名	NIS+ V3 クライアントのドメイン名
65	NIS+ V3 サーバ アドレス	NIS+ V3 サーバのアドレス
66	TFTP サーバ名	TFTP サーバ名
67	ブート ファイル名	ブート ファイル名
68	ホーム エージェント アドレス	モバイル IP ホーム エージェントのアドレス
69	Simple Mail サーバ アドレス	Simple Mail Transfer Protocol (SMTP) サーバのアドレス
70	Post Office サーバ アドレス	Post Office Protocol (POP3) サーバのアドレス
71	Network News サーバ アドレス	Network News Transfer Protocol (NNTP) サーバのアドレス
72	WWW サーバ アドレス	WWW サーバのアドレス
73	Finger サーバ アドレス	Finger サーバのアドレス
74	Chat サーバ アドレス	Chat サーバのアドレス
75	StreetTalk サーバ アドレス	StreetTalk サーバのアドレス
76	StreetTalk Directory Assistance アドレス	StreetTalk Directory Assistance (STDA) サーバのアドレス
77	ユーザ クラス情報	ユーザ クラス情報
78	SLP ディレクトリ エージェント	Service Location Protocol (SLP) ディレクトリ エージェントのアドレス
79	SLP サービス スコープ	Service Location Protocol (SLP) エージェントのスコープ
80	急速コミット	急速コミットの使用

オプション番号	名前	説明
81	FQDN、完全修飾ドメイン名	完全修飾ドメイン名
82	リレー エージェント情報	リレー エージェント情報
83	インターネット ストレージ ネーム サービス	Internet Storage Name Service (iSNS) サーバのアドレス
84	Undefined	該当なし
85	Novell ディレクトリ サービス	Novell Directory Services (NDS) サーバのアドレス
86	Novell Directory サーバ ツリー名	Novell Directory Services (NDS) サーバ ツリー名
87	Novell Directory サーバ コンテキスト	Novell Directory Services (NDS) サーバ コンテキスト
88	BCMCS コントローラドメイン名リスト	Broadcast/Multicast Services (BCMCS) コントローラのドメイン名リスト
89	BCMCS コントローラ IPv4 アドレス リスト	BCMCS コントローラの IPv4 アドレス リスト
90	認証	認証
91 – 92	Undefined	該当なし
93	クライアント システム	クライアントのシステム手法の種類
94	クライアント ネットワーク装置インターフェース	クライアントのネットワーク装置インターフェースの種類
95	LDAP 利用	Lightweight Directory Access Protocol (LDAP) の使用
96	Undefined	該当なし
97	UUID/GUID ベースのクライアント識別子	UUID/GUID に基づくクライアント識別子
98	オープン グループのユーザ認証	オープン グループのユーザ認証サービスの URL
99 – 108	Undefined	該当なし
109	自律システム番号	自律システム番号
110 – 111	Undefined	該当なし
112	NetInfo Parent アドレス	NetInfo Parent サーバのアドレス
113	NetInfo Parent サーバ タグ	NetInfo Parent サーバのタグ
114	URL:	URL
115	Undefined	該当なし
116	自動構成	DHCP 自動設定
117	ネーム サービス検索	ネーム サービス検索
118	サブネット コレクション	サブネットの選択
119	DNS ドメイン検索リスト	DNS ドメイン検索リスト
120	SIP サーバ DHCP オプション	Session Initiation Protocol (SIP) サーバのドメイン名またはアドレス
121	クラスレス静的ルート オプション	クラスレス静的ルート オプション

オプション番号	名前	説明
122	CCC, CableLabs クライアント構成	CableLabs クライアントの構成オプション
123	GGeoConf	GGeoConf
124	Vender-Identifying ベンダー クラス	ベンダー識別のためのベンダー種別情報
125	Vender-Identifying ベンダー 固有	ベンダー識別のためのベンダー固有情報
126 – 127	Undefined	該当なし
128	TFTP サーバ IP アドレス	IP 電話のソフトウェアを読み込むための TFTP サーバの IP アドレス
129	コール サーバ IP アドレス	コールサーバの IP アドレス
130	差別文字列	ベンダーを識別するための差別文字列
131	リモート統計サーバ IP アドレス	リモート統計サーバの IP アドレス
132	802.1Q VLAN ID	IEEE 802.1Q の VLAN ID
133	802.1Q L2 優先順位	IEEE 802.1Q の第 2 層優先順位
134	Diffserv コード ポイント	VoIP シグナルとメディア ストリームのための Diffservコード ポイント
135	電話アプリケーションの HTTP プロキシ	電話固有アプリケーション用の HTTP プロキシ
136 – 149	Undefined	該当なし
150	TFTP サーバ アドレス, イーサブート, GRUB 構成	TFTP サーバのアドレス、イーサブート、GRUB 構成
151 – 174	Undefined	該当なし
175	イーサブート	イーサブート
176	IP 電話	IP 電話
177	イーサブート、PacketCable および CableHome	イーサブート、PacketCable および CableHome
178 – 207	Undefined	該当なし
208	pxelinux.magic (文字列) = 241.0.116.126	pxelinux.magic (文字列) = 241.0.116.126
209	pxelinux.configfile (テキスト)	pxelinux.configfile (テキスト)
210	pxelinux.pathprefix (テキスト)	pxelinux.pathprefix (テキスト)
211	pxelinux.reboottime	pxelinux.reboottime
212 – 219	Undefined	該当なし
220	サブネット割り当て	サブネットの割り当て
221	仮想サブネット割り当て	仮想サブネットの選択
222 – 223	Undefined	該当なし
224 – 257	プライベート利用	プライベート利用

RFC で定義された DHCPV6 オプション番号

オプション番号	名前	説明
12	サーバ ユニキャスト	ホスト名の文字列 ((サーバ ユニキャスト) など)
21	SIP サーバ ドメイン名リスト	SIP サーバ ドメイン名のリストを有効にする
22	SIP サーバ IPv6 アドレス リスト	SIP サーバ IPv6 アドレスのリストを有効にする
23	DNS 再帰名前サーバ	DNS 再帰名前サーバのリストを有効にする
24	ドメイン検索リスト	検索用ドメイン名のリストを有効にする
27	ネットワーク情報サービス (NIS) サーバ	ネットワーク情報サービス (NIS) サーバのリストを有効にする
28	ネットワーク情報サービス V2 (NIS+) サーバ	ネットワーク情報サービス V2 (NIS+) サーバのリストを有効にする
29	ネットワーク情報サービス (NIS) ドメイン名	ネットワーク情報サービス (NIS) ドメイン名のリストを有効にする
30	ネットワーク情報サービス V2 (NIS+) ドメイン名	ネットワーク情報サービス V2 (NIS+) ドメイン名のリストを有効にする
31	シンプル ネットワーク タイム プロトコル (SNTP) サーバ	シンプル ネットワーク タイム プロトコル (SNTP) サーバのリストを有効にする
32	情報更新時間	情報更新時間

DHCP オプション オブジェクトの編集

マウス カーソルを編集したい DHCP オプション オブジェクトに重ね、「**編集**」アイコンをクリックします。構成の設定は、「**DHCP オプション オブジェクトの追加**」ダイアログと同じです。詳細については、「DHCP オプション オブジェクトの設定」を参照してください。

DHCP オプション オブジェクトの「**名前**」は変更できません。

DHCP オプション オブジェクトの削除

DHCP オプション オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > DHCP オプション**」ページに移動します。
2. 以下のいずれかを実行します。

- マウス カーソルを削除したい DHCP オプションに重ね、**削除**アイコンをクリックします。
- 削除する 1 つ以上のオブジェクトのチェックボックスをクリックし、ページ上部の**削除**アイコンをクリックします。

6

AWS

AWS のオブジェクトやグループをセットアップする前に、そこで必要とされる AWS 資格情報を使用してファイアウォールを構成してください。これらの構成は、「**ネットワーク > システム > AWS 構成**」ページで行うことができます。さらに、「設定のテスト」ボタンを使用して、設定を確認してから作業を進めてください。詳細については、『*SonicOS システム セットアップ*』管理ガイドの「*AWS 資格情報の設定*」を参照してください。

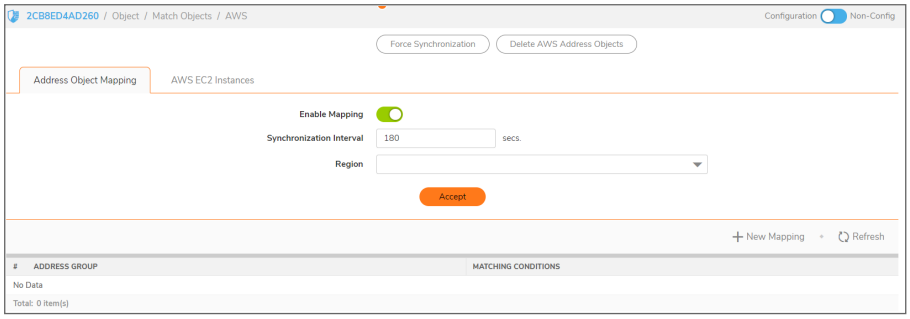
AWS がまだ構成されていない場合は、「**オブジェクト > プロファイル オブジェクト > AWS**」ページに構成ページへのリンクが表示されます。これをクリックすると、「**ネットワーク > システム > AWS 設定**」ページが開きます。

AWS オブジェクト

「**AWS**」ページを使用すると、AWS クラウドで実行している EC2 インスタンスの IP アドレスをファイアウォールで構成したアドレス オブジェクトやアドレス グループにマッピングできます。

インスタンスの IP アドレスに対して新規のアドレス オブジェクトが作成され、インスタンスのすべてのアドレスに対してアドレス グループが作成されます。これらのインスタンス アドレス グループを既存のアドレス グループに追加できます。これらのオブジェクトは、他のアドレス オブジェクトやアドレス グループと同様に、ファイアウォールのポリシーや機能でアクセスの許可/遮断やトラフィックのルーティングのために使用できます。

「**プロファイル オブジェクト > AWS オブジェクト**」ページで、SonicOS 管理者は EC2 インスタンスのプロパティ セットを指定できます。監視対象のいずれかのリージョンにプロパティ セットと一致するインスタンスがあれば、そのインスタンスを表すアドレスグ ループが関連マッピングで指定した既存のカスタム アドレス グループに有効に追加されるようにアドレス オブジェクトやアドレス グループが作成されます。このアドレス グループをファイアウォールのポリシーで使用すれば、AWS で実行される EC2 インスタンスとのインタラクションがこれらのポリシーによって実現されます。



トピック:

AWS によるアドレス オブジェクト割り当てについて

EC2 インスタンスは、AWS 上で動作する仮想マシン (VM) です。インスタンスにはいくつかの種類があり、顧客がインスタンスに求めるリソースに応じて、各インスタンスをそのうちの 1 つにすることができます。仮想マシンは特定の Amazon Machine Image (AMI) のインスタンスであり、本質的には、そこから作成される VM のテンプレートおよび仕様です。すべての EC2 インスタンスには、以下を含む多数のプロパティがあります。

- インスタンス種別
- 作成に使われた AMI
- 実行状態
- 識別に使われる ID
- インスタンスの配置先の仮想プライベート クラウド (VPC) の ID
- ユーザ定義タグのセット

これらのプロパティの一部またはすべてを使用して、対応するインスタンスを、SonicOS 管理者が以前にファイアウォール上で構成したアドレス グループにマッピングできます。これらのアドレス グループをルート、VPN、およびファイアウォールのポリシーで使用して、ファイアウォールと AWS ホスト マシンとのインタラクションに影響を与えることができます。

EC2 インスタンスをファイアウォールのアドレス グループにマッピングするために、管理者はインスタンスのプロパティ セットと既存のアドレス グループの間で任意の数のマッピングを構成します。監視対象のいずれかの AWS リージョンで、指定したプロパティ セットと一致する EC2 インスタンスがある場合、そのインスタンスを表す 1 つ以上のアドレス オブジェクトと 1 つのアドレス グループが作成され、そのアドレス グループが関連マッピングのマッピング先アドレス グループに追加されます。

EC2 インスタンスは、仮想ネットワーク インターフェースの数と Elastic IP アドレスを使うかどうかに応じて、複数のプライベート IP アドレスとパブリック IP アドレスを持つことができます。インスタンスがマッピングで指定されたプロパティと一致する場合、アドレス オブジェクトは、パブリックとプライベートの両方の IP アドレスごとに作成されます。これらのアドレス オブジェクトは、EC2 インスタンス全体を表す 1 つのアドレス グループに追加されます。これが「インスタンス アドレス グループ」として、マッピング先のアドレス グループ (つまり、ファイアウォールのさまざまな

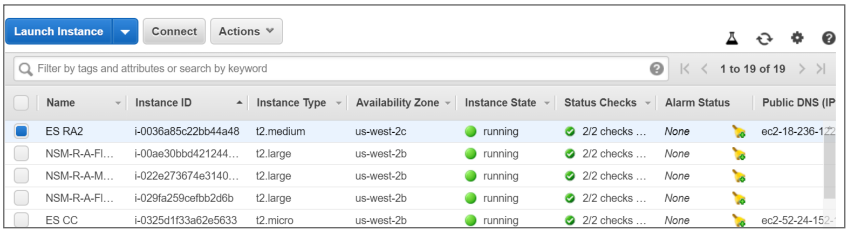
ポリシー構成で使われる既存のアドレス グループ) に追加されます。いずれか 1 つの EC2 インスタンスが複数のマッピング条件に一致することがあります。その場合、インスタンス アドレス グループは複数のマッピング先アドレス グループに追加されます。その数に制限はありません。

AWS 上の EC2 インスタンスのタグ付け

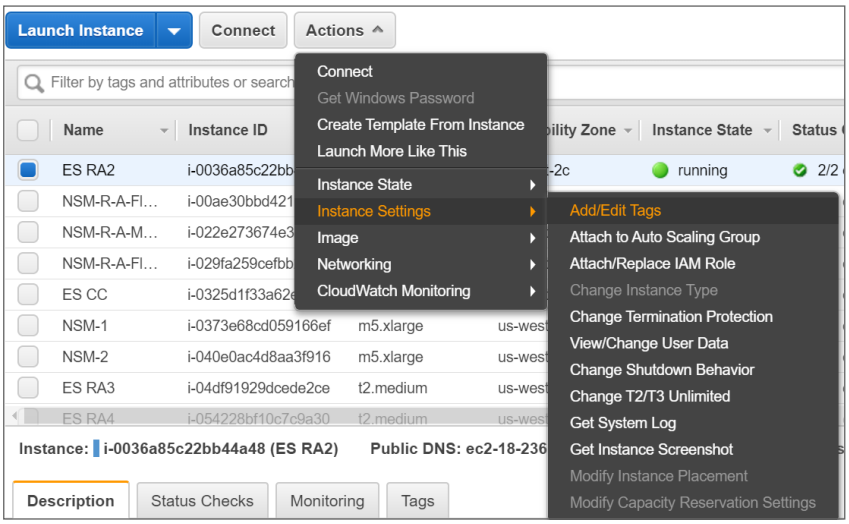
EC2 インスタンスのタグ付けは、いくつか方法があります。ここでは、手動による方法を説明します。

既存の EC2 インスタンスに手動でタグを追加するには、以下の手順に従います

1. AWS コンソールで EC2 ダッシュボードに移動し、「インスタンス」ページを表示します。
2. テーブルの最初の列にあるチェックボックスをオンにして、タグを付けたいインスタンスを選択します。

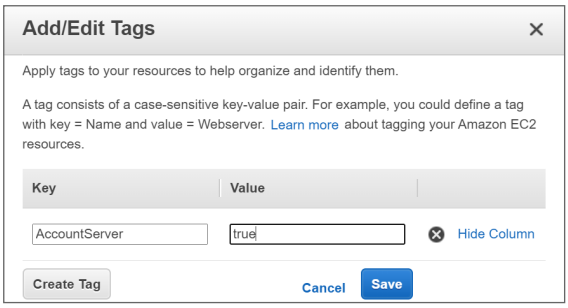


3. 選択したインスタンスで、「**動作**」ボタンをクリックしてポップアップ メニューを開きます。
4. 「**インスタンス設定**」を選択し、「**タグの追加/編集**」を選択します。

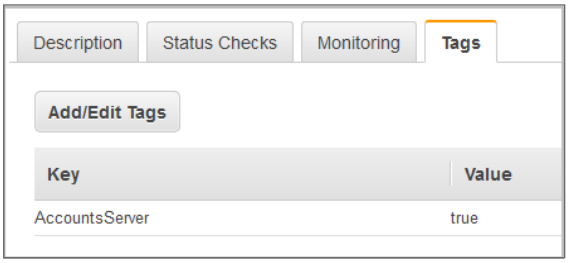


「**タグの追加/編集**」ダイアログが表示されます。

5. 「**タグの追加/編集**」ダイアログで、説明となる値を「**鍵**」および「**値**」フィールドに入力します。



6. 「**保存**」を選択して、このキーと値でインスタンスにタグ付けします。
7. EC2 ダッシュボード の「インスタンス」ページでタグを確認します。インスタンスが選択された状態で、ページの下部にあるパネルの「**タグ**」タブを選択して、関連するタグを表示します。これにより、EC2 インスタンスにタグが付いていることが確認できます。

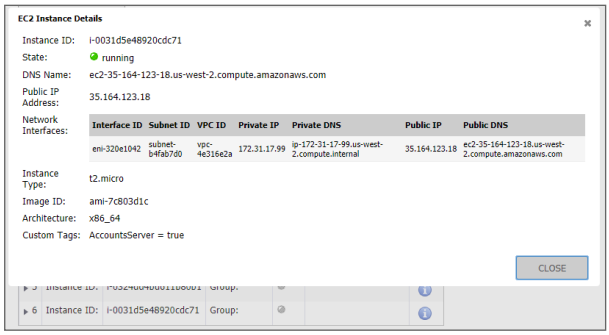


SonicOS 管理インターフェースでアドレス オブジェクトのマッピングを定義するときに、このタグを使用できるようになりました。

SonicOS でのインスタンス プロパティの表示

「**プロファイル オブジェクト > AWS**」ページでは、EC2 インスタンスのプロパティ セットとファイアウォールのアドレス グループの間でマッピングを定義することができます。指定したプロパティ セットに一致する EC2 インスタンスに対してアドレス オブジェクトとアドレス グループが作成され、アドレス グループはマッピング先のアドレス グループに追加されます。

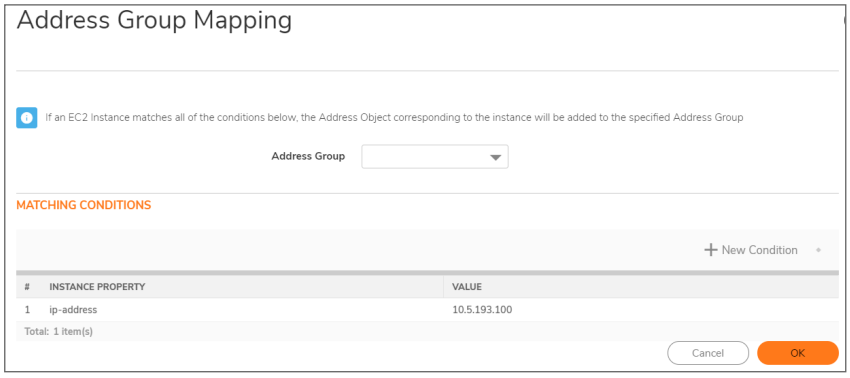
任意の EC2 インスタンスで、インスタンスの行にある「**情報**」ボタンをクリックすると、マッピングで使用できるさまざまなプロパティの値を表示できます。これにより、インスタンスの ID 、実行状態、AMI、種別、VPC ID、各種 IP アドレスなど、さまざまなプロパティを示すポップアップ ダイアログが表示されます。ユーザ定義タグやカスタム タグと、それらの値もリストされます。



新規のアドレス オブジェクト割り当ての作成

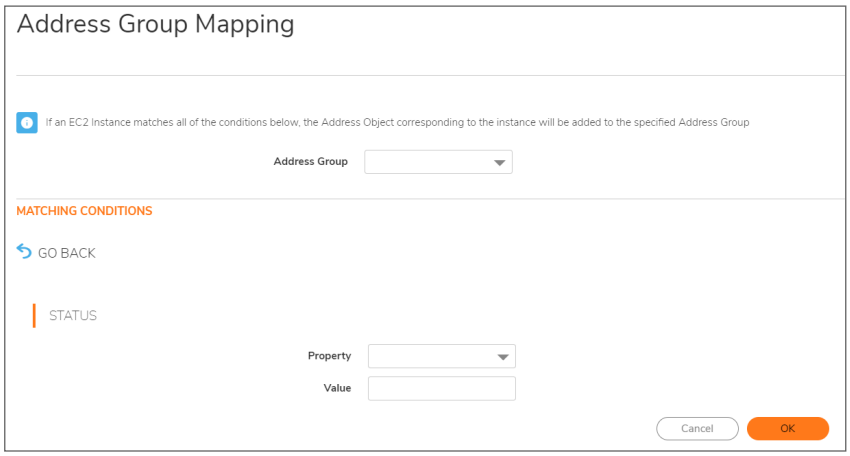
新しいアドレス オブジェクト割り当てを作成するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > AWS**」ページに移動します。
2. 「**新しい割り当て**」ボタンをクリックします。表示されたダイアログで、このマッピングの詳細を指定できます。



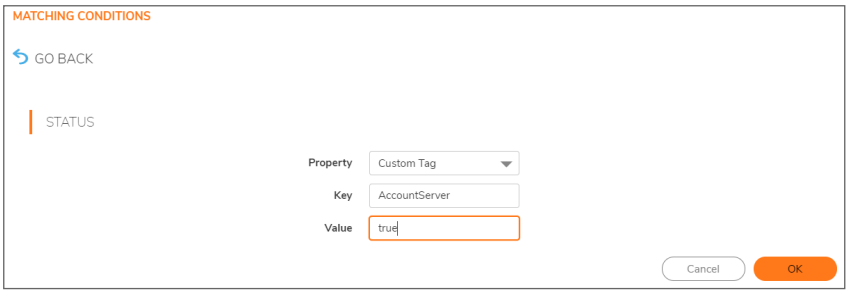
3. 「**アドレス グループ**」ドロップダウン リストで、一致する EC2 インスタンスを表すアドレスグループの追加先となる既存のアドレス グループを選択します。

   カスタム アドレス グループのみが選択コントロールに表示されます。カスタム タグがアドレス グループに追加してある場合は、このカスタム タグを使用して新しい条件をマッピングに追加できます。
4. 「**新しい条件**」ボタンをクリックします。「割付条件」オプションが表示されます。

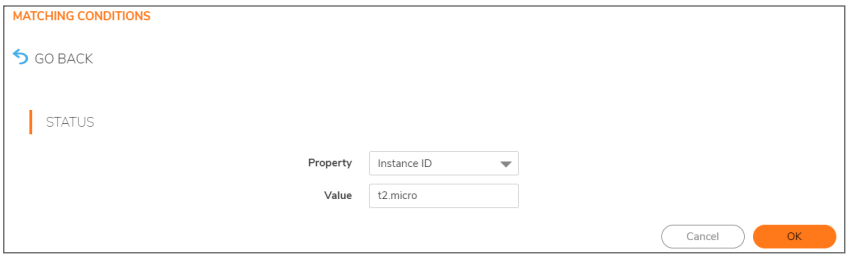


5. 「**プロパティ**」ドロップダウン リストから目的のプロパティを選択します。たとえば、「**ユーザ定義タグ**」を選択します。
6. 「**キー**」フィールドに、タグのキーを入力します。

7. 「**値**」フィールドに、true など、照合したい値を入力します。



8. 「**OK**」をクリックします。
9. 「**アドレス グループ割り当て**」ダイアログに戻り、必要に応じて「**新しい条件**」ボタンを再度クリックして別のマッピング条件を追加します。
10. 「**プロパティ**」ドロップダウン リストから目的のプロパティを選択します。
11. 表示されたフィールドに必要に応じて値を入力します。



12. 「**OK**」をクリックします。
13. 「**アドレス グループ割り当て**」ダイアログに戻り、作成しようとしているマッピング条件の全体を確認します。関心のあるリージョンに指定の条件 (この例では、カスタム タグ *AccountsServer = true*、種別 *t2.micro*) と一致する EC2 インスタンスがある場合、そのインスタンスに対して IP アドレスごとにアドレス オブジェクトが作成されます。これらのアドレス オブジェクトは、EC2 インスタンス全体を表すアドレス グループに追加され、そのアドレス グループはマッピング先のアドレス グループに追加されます。この例では、*AccountsDeptServers* というアドレス グループです。
14. 必要に応じて、行の「**管理**」列にある対応するボタンをクリックして、特定の条件を編集または削除します。
15. 準備ができたら、「**OK**」をクリックします。
16. 「**オブジェクト > プロファイル オブジェクト > AWS**」ページで、「**適用**」をクリックしてこの割り当てを保存します。

割り当てを有効にする

アドレス オブジェクトのマッピングはいくつでも作成できますが、有効にするまで効力を持ちません。

割り当てを有効にするには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > AWS**」ページで、「**割り当てを有効にする**」オプションを選択します。
2. 「**適用**」ボタンを選択します。

同期の設定

「**同期間隔**」は、ファイアウォールがどれくらいの頻度で変更を確認し、関連するアドレス オブジェクトとアドレス グループに対して必要な更新を行うかを決定します。

同期が必要な理由は、アドレス オブジェクトのマッピングや監視対象の AWS リージョンはいつでも変更または再構成される可能性があり、AWS 上で EC2 インスタンスの IP アドレスと実行状態が変化するかもしれないからです。

同期間隔を構成するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > AWS**」ページで、「**同期間隔**」フィールドに必要な秒数を入力します。
2. 「**適用**」を選択します。

同期を強制するには、以下の手順に従います

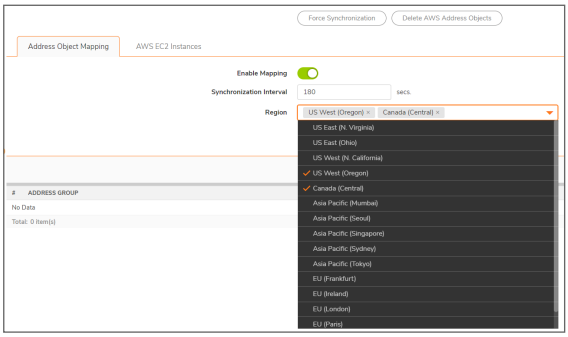
1. 「**オブジェクト > プロファイル オブジェクト > AWS**」ページで、「**同期の強制**」または「**AWS アドレス オブジェクトの削除**」ボタンをクリックします。
   これは、変更に気づいたときに更新後のアドレス オブジェクトを急いで確認したい場合に便利です。
2. 「**適用**」を選択します。
3. 「**再表示**」ボタンをクリックして、ページに最新のデータが反映されるようにします。

監視するリージョンの設定

EC2 インスタンスは特定の AWS リージョンに関連付けられています。SonicOS は、特に関心のある AWS リージョンのみを監視します。既定で、この設定は AWS の設定時に「既定のリージョン」として選択した AWS リージョンに初期化され、ファイアウォールのログを AWS CloudWatch ログに送信する場合に使用されます。ただし、複数のリージョンを監視対象として選択することも可能で、その場合、マッピングは選択したリージョンごとに適用されます。

1 つ以上のリージョンを監視対象として選択するには、以下の手順に従います

1. 「**オブジェクト > プロファイル オブジェクト > AWS**」ページで、「**地域**」ドロップダウン リストをクリックし、関心のある各リージョンのチェックボックスをオンにします。



2. 「**適用**」を選択します。

AWS アドレス オブジェクトとアドレス グループの確認

マッピングを適切に行うことによって、「**同期間隔**」を設定し、「**リージョン**」を指定し、最も重要な「**割付**」を有効にすると、一致する EC2 インスタンスとその IP アドレスを表すアドレス オブジェクトおよびアドレス グループを表示できます。

たとえば、「AWS」ページの「EC2 インスタンス」テーブルには、そのアドレス グループと、割付先の各アドレス グループが表示されます。

関連する行を展開すると、インスタンスのパブリックおよびプライベート IP アドレスに対応するアドレス オブジェクトを表示できます。

SonicOS の「**オブジェクト > 一致オブジェクト > アドレス**」ページに移動し、「アドレス オブジェクト」画面を表示すると、同じホストのアドレス オブジェクトが表示されます。VPNはプライベート IP アドレスのゾーンで使用され、WANはパブリック アドレス ゾーンとして使用されます。

インスタンスのアドレス グループと IP アドレスごとにあるアドレス オブジェクトには一定の命名規則が適用されます。それはインスタンス ID をベースとし、アドレス オブジェクトの場合はアドレスがパブリックかプライベートかによって異なる接尾辞が使用されます。

「**アドレス グループ**」画面を表示し、関心のある行を展開すると、元の *AccountsDeptServers* アドレス グループに EC2 インスタンスを表すアドレス グループがメンバーとして表示されます。

EC2 インスタンスのアドレス グループには、その IP アドレスごとに作成されたアドレス オブジェクトが含まれています。

7

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます:
https://www.sonicwall.com/ja-jp/support

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS プロファイル オブジェクト 管理者ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005640-10 Rev B

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、「SonicWall Inc.」を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035