SonicOS および SonicOSX 7 ネットワーク DNS

管理ガイド

SONICWALL®

目次

1

DNS の設定

補足: SonicOS/X という表記は、その機能が両方の SonicOS および SonicOSX で使用可能なことを示します。

ドメイン ネーム システム (DNS) は、覚えにくい数値の IP アドレスではなく、完全修飾ドメイン (FQDN) と呼ばれる英数字の名前を使ってインターネット上のホストを識別する、分散型の階層システムです。「**ネットワーク > DNS**」では、必要に応じて DNS 設定を手動で構成できます。

「**ネットワーク > DNS**」のオプションは、「**IPv6**」と「**IPv4**」のどちらを選択するかによって異なります。

IP バージョンを選択するには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 「**IPv4**」タブまたは「**IPv6**」タブを選択します。

トピック:

- IPv4 の DNS 設定
- IPv6 の DNS 設定
- 分割 DNS 用のドメイン固有 DNS サーバの設定

IPv4 の DNS 設定

「**ネットワーク > DNS > IPv4**」ページには、以下のセクションがあります。

- 使用する DNS サーバの指定
- 分割 DNS サーバのプロキシを有効にする
- DNS 再割り当て攻撃の防御
- FQDN に対する DNS の割り当て
- 「TCP を介した FQDN 用 DNS ホスト名検索」の有効化
- DNS キャッシュ

使用する DNS サーバの指定

IP バージョンに関係なく、SonicOS/X による DNS サーバの選択方法を指定できます。この方法はどちらの IP バージョンでも同じです。

使用する DNS サーバを指定するには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 選択したバージョンに従って「**IPv4 DNS 設定**」または「**IPv6 DNS 設定**」セクションで、次のいずれかを選択します。
   - 手動で DNS サーバを指定するには、以下の手順に従います。
     1. 「**手動で DNS サーバを指定する**」を選択します。
     2. 「**DNS サーバ**」フィールドに IP アドレスを最大 3 つ入力します。
   - WAN ゾーン用に構成された DNS 設定を使用するには、「**WAN ゾーンと同じDNSサーバ 設定にする**」を選択します。このオプションは既定の設定です。「**DNS サーバ**」フィールドに、IP アドレスが自動的に入力されます。
3. 「**IPv6**」を選択した場合に、IPv6 サーバのみを使用するには、「**IPv6 DNS サーバ優先**」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。

   SonicOS/X DNS は、次の種類のサーバをサポートしています。
   - DNS_SYSTEM_BEHAVIOR – システムの既定の動作。このオプションの設定に依存します。
   - DNS_PREFER_V4_DNSSERVER – 障害が発生しない限り IPv4 DNS サーバを優先し、障害が発生した場合に IPv6 DNS サーバを要求します。
   - DNS_PREFER_V6_DNSSERVER – 障害が発生しない限り IPv6 DNS サーバを優先し、障害が発生した場合に IPv4 DNS サーバを要求します。

   △ | **注意: IPv6 DNS サーバを適切に設定済みである場合に限り、このオプションを選択してください。**
4. 「**適用**」を選択して変更を保存します。

分割 DNS サーバのプロキシを有効にする

分割 DNS サーバのプロキシを有効にするには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 「**分割 DNS**」セクションまでスクロールします。
3. 「**分割 DNS サーバのプロキシを有効にする**」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す。
4. 「**適用**」をクリックします。

DNS 再割り当て攻撃の防御

DNS 再割り当ては、ウェブ ページに埋め込まれたコードに対する DNS ベースの攻撃です。通常、ウェブ ページに埋め込まれたコード (JavaScript、Java、および Flash) からの要求は、その発信元のウェブ サイトにバインドされます (「同一発信元ポリシー」を参照)。DNS 再割り当て攻撃によって、プライベート ネットワークに侵入する JavaScript ベースのマルウェアの能力が高められ、ブラウザの同一発信元ポリシーが覆されることがあります。

DNS 再割り当て攻撃者は、自らが制御する DNS サーバに委託されるドメインを登録します。このサーバは、非常に短い持続時間 (TTL) パラメータで応答するように設定されているため、結果がキャッシュされません。最初の応答には、悪意のあるコードをホストしているサーバの IP アドレスが含まれます。その後の要求には、プライベート (RFC 1918) ネットワークからの IP アドレスが含まれます。このネットワークはおそらくファイアウォールの後ろにあり、攻撃者のターゲットになります。どちらも完全に有効な DNS 応答であるため、これによってサンドボックス スクリプトにプライベート ネットワーク内のホストへのアクセスが許可されます。このような短期的ながら有効な DNS 応答でアドレスを繰り返すことによって、スクリプトがネットワーク内をスキャンし、他の悪意ある動作を実行することができます。

DNS 再割り当て攻撃の防御を設定するには、以下の手順を実行します。

1. 「**ネットワーク > DNS 設定**」に移動します。
2. 「**DNS 再割り当て攻撃の防御**」セクションまでスクロールします。
3. 「**DNS 再割り当て攻撃の防御を有効にする**」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。2 つのオプションが使用可能になります。
4. 「**動作**」から、DNS 再割り当て攻撃が検知されたときに実行する動作を選択します。
   - **攻撃をログする** (既定)
   - **攻撃をログし、クエリ拒否応答を返す**
   - **攻撃をログし、DNS 応答を破棄する**
5. 「**許可ドメイン**」から、許可するドメイン名を含む FQDN アドレス オブジェクトや FQDN アドレス オブジェクト グループ (`*.SonicWall.com` など) を選択します。これらのオブジェクトやオブジェクト グループについては、ローカルに接続/ルーティングされるサブネットを正当な応答と見なします。

   「**FQDN アドレス オブジェクト グループを作成する...**」または「**FQDN アドレス オブジェクトを作成する...**」を選択して、新しい FQDN アドレス オブジェクトや FQDN アドレス オブジェクト グループを作成することもできます。
6. 「**適用**」をクリックします。

FQDN に対する DNS の割り当て

FQDN に対する DNS の割り当てを有効にするには、以下の手順に従います。

1. 「**ネットワーク > DNS 設定**」に移動します。
2. 「**FQDN に対する DNS の割り当て**」セクションまでスクロールします。
3. 「**FQDN オブジェクトは承認済みサーバからの DNS 応答のみをキャッシュする**」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。
4. 「**適用**」を選択します。

「TCP を介した FQDN 用 DNS ホスト名検索」の有効化

既定では、DNS クエリは UDP で送信されます。応答の長さが UDP で許可される最大値を超える場合、DNS の応答に Truncated（切り捨て）フラグが含まれる場合があります。

「**TCP を介した FQDN 用 DNS ホスト名検索を有効にする**」オプションが

- 有効化されていて、DNS の応答に Truncated フラグが設定されている場合、SonicOS/X は、追加の DNS クエリを TCP で送信し、複数の IP アドレスに対して完全な DNS 応答を決定します。
- このオプションが無効の場合、DNS クエリは UDP で送信され、SonicOS/X は、応答に Truncated フラグの設定があっても DNS 応答のパケットに含まれる IP アドレスの処理のみを行います。

TCP による DNS 応答を DNS サーバから受信できない場合、DNS クエリは 1 秒後にタイムアウトします。

このオプションは、セキュリティ装置が UDP 経由で DNS 応答を受信している間に、FQDN から TCP を介して DNS クエリを送信するとき、より多くの IP アドレスを取得するために使用されます。

TCP を介した FQDN 用 DNS ホスト名検索を有効化するには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 「**TCP を介した FQDN 用 DNS ホスト名検索**」セクションまでスクロールします。
3. 「**TCP を介した FQDN 用 DNS ホスト名検索を有効にする**」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。
4. 「**適用**」を選択します。

DNS キャッシュ

通常 DNS キャッシュの内容を表示するには、「**DNS キャッシュの表示**」を選択します。ポップアップにキャッシュの内容が表示されます。

対象	DNS サーバ名: • 正引き DNSキャッシュ、ホスト名。 • 逆引き DNS キャッシュ、IP アドレスの文字列表現。
DNS 名	www.SonicWall.com などのドメイン名、または IP アドレス。
IP アドレス	解決結果 IP アドレス
TTL（秒）	持続時間（TTL）。DNS 応答からの TTL 値。
消去	選択すると、サーバの DNS キャッシュ エントリが消去されます。
すべて消去	選択すると、表示されているすべてのサーバのすべての DNS キャッシュ エントリが消去されます。

IPv6 の DNS 設定

「**ネットワーク > DNS > IPv6**」ページには、以下のセクションがあります。

使用する DNS サーバの指定

IP バージョンに関係なく、SonicOS/X による DNS サーバの選択方法を指定できます。この方法はどちらの IP バージョンでも同じです。

使用する DNS サーバを指定するには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 選択したバージョンに従って「**IPv4 DNS 設定**」または「**IPv6 DNS 設定**」セクションで、次のいずれかを選択します。
    - 手動で DNS サーバを指定するには、以下の手順に従います。
        1. 「**手動で DNS サーバを指定する**」を選択します。
        2. 「**DNS サーバ**」フィールドに IP アドレスを最大 3 つ入力します。
    - WAN ゾーン用に構成された DNS 設定を使用するには、「**WAN ゾーンと同じDNSサーバ 設定にする**」を選択します。このオプションは既定の設定です。「**DNS サーバ**」フィールドに、IP アドレスが自動的に入力されます。
3. 「**IPv6**」を選択した場合に、IPv6 サーバのみを使用するには、「**IPv6 DNS サーバ優先**」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。

    SonicOS/X DNS は、次の種類のサーバをサポートしています。
    - DNS_SYSTEM_BEHAVIOR – システムの既定の動作。このオプションの設定に依存します。
    - DNS_PREFER_V4_DNSSERVER – 障害が発生しない限り IPv4 DNS サーバを優先し、障害が発生した場合に IPv6 DNS サーバを要求します。
    - DNS_PREFER_V6_DNSSERVER – 障害が発生しない限り IPv6 DNS サーバを優先し、障害が発生した場合に IPv4 DNS サーバを要求します。

    △ | **注意: IPv6 DNS サーバを適切に設定済みである場合に限り、このオプションを選択してください。**
4. 「**適用**」を選択して変更を保存します。

分割 DNS サーバのプロキシを有効にする

分割 DNS サーバのプロキシを有効にするには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 「**分割 DNS**」セクションまでスクロールします。
3. 「**分割 DNS サーバのプロキシを有効にする**」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す。
4. 「**適用**」をクリックします。

「TCP を介した FQDN 用 DNS ホスト名検索」の有効化

既定では、DNS クエリは UDP で送信されます。応答の長さが UDP で許可される最大値を超える場合、DNS の応答に Truncated（切り捨て）フラグが含まれる場合があります。

「**TCP を介した FQDN 用 DNS ホスト名検索を有効にする**」オプションが

- 有効化されていて、DNS の応答に Truncated フラグが設定されている場合、SonicOS/X は、追加の DNS クエリを TCP で送信し、複数の IP アドレスに対して完全な DNS 応答を決定します。
- このオプションが無効の場合、DNS クエリは UDP で送信され、SonicOS/X は、応答に Truncated フラグの設定があっても DNS 応答のパケットに含まれる IP アドレスの処理のみを行います。

TCP による DNS 応答を DNS サーバから受信できない場合、DNS クエリは 1 秒後にタイムアウトします。

このオプションは、セキュリティ装置が UDP 経由で DNS 応答を受信している間に、FQDN から TCP を介して DNS クエリを送信するとき、より多くの IP アドレスを取得するために使用されます。

TCP を介した FQDN 用 DNS ホスト名検索を有効化するには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 「**TCP を介した FQDN 用 DNS ホスト名検索**」セクションまでスクロールします。
3. 「**TCP を介した FQDN 用 DNS ホスト名検索を有効にする**」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。
4. 「**適用**」を選択します。

分割 DNS 用のドメイン固有 DNS サーバの設定

必要に応じて、個別のドメイン固有 DNS サーバを設定することができます。

ドメイン名	DNS サーバの名前。
DNS サーバ	DNS サーバの IPv4/IPv6 IP アドレス。 ⓘ **補足:** DNS サーバの状況は、「**ネットワーク > DNS プロキシ**」ページに表示されます。
ローカル インターフェース	DNS サーバに割り当てられているインターフェース
構成	各サーバについて**編集**アイコンと**削除**アイコンが表示されます。

トピック:

- 分割 DNS について
- 分割 DNS サーバのプロキシを有効にする
- 分割 DNS サーバの追加
- 分割 DNS エントリの編集
- 分割 DNS エントリの削除

分割 DNS について

分割 DNS は、一連のサーバを設定してそれらを特定のドメイン名（ワイルドカードも使用可能）に関連付けられるようにする拡張機能です。SonicOS/X がドメイン名と一致するクエリを受信すると、指定された DNS サーバにその名前が送信されます。

例えば、2 台のファイアウォールがネットワークに接続されたトポロジがあるとします。

- 1 台のファイアウォールはインターネットに接続されています。
- もう 1 台は企業ネットワークに接続された VPN トンネルです。
- 既定の DNS クエリはパブリック ISP の DNS サーバに送信されます。
- `*.SonicWall.com` に対するすべてのクエリは、VPN トンネルの背後にある DNS サーバに送信されます。

分割 DNS エントリの表示と設定に関する参照先:「分割 DNS 用のドメイン固有 DNS サーバの設定」。

分割 DNS エントリを追加すると、`SonicWall.com` に対するすべてのクエリは特定のサーバに送信されます（参照先:「分割 DNS 用のドメイン固有 DNS サーバの設定」）。

複数の DNS サーバを、`SonicWall.com` に対するクエリを処理するように設定することもできます。

トピック:

- パーティションごとの DNS サーバと分割 DNS について

パーティションごとの DNS サーバと分割 DNS について

認証パーティションの有無に関係なく、通常はドメイン独自の DNS サーバを使用してそのドメイン内にある機器の名前を解決する必要があります。また、ときには異なる外部 DNS サーバを使用した外部ホスト名の解決が必要になることもあります。複数の認証パーティションがある場合はさらに複雑になります。通常、複数のパーティション内のホスト名を解決するには複数の DNS サーバを使用する必要があるからです。

ⓘ **補足:** 通常、LDAPでは、LDAP サーバが IP アドレスによって設定されていても DNS 名で参照先サーバを示すため、ドメイン独自の DNS サーバの使用が予期せず必要となる場合があります。

また、異なる外部 DNS サーバを使用した外部ホスト名の解決が必要になる例として、内部ドメインの DNS サーバでは解決できない外部使用クラウド サービスが関係している場合があります。

分割 DNS 機能を SonicWall ネットワーク セキュリティ装置から直接使用するのは、ドメイン内の機器の名前を解決するとき DNS プロキシを有効化する必要がない場合です。たとえば、関連性のない複数のドメインで認証パーティション処理を行う場合などが該当します。

分割 DNS で設定された DNS サーバ（「分割 DNS 用のドメイン固有 DNS サーバの設定」を参照）は、次のように、内部ドメイン内のホスト名の DNS 検索に直接使用されます。

- これは、ネットワーク セキュリティ装置のメイン DNS キャッシュ内にエントリのあるすべてに適用されます。
    - SMTP サーバ
    - Syslog サーバ
    - ウェブ プロキシ サーバとユーザ (内部) プロキシ サーバ
    - GMS と GMS スタンバイ
    - POP サーバ
    - RADIUS 認証サーバとアカウント サーバ
    - LDAP サーバ
    - SSO / ターミナル サービス エージェントと RADIUS アカウント クライアント
- パーティション処理が有効になっていて、1 つのパーティションに 1 つのドメインまたは親/サブドメインの 1 つのツリー (1 つの AD フォレスト) が割り当てられている場合、パーティションの最上位ドメインに分割 DNS サーバを設定すると、それらは内部パーティション構造にコピーされます。それらの DNS サーバは、パーティション内のエージェント、サーバ、クライアントの名前の解決に使用されます。
- パーティション処理が有効になっていて、1 つのパーティションに複数の別個のドメインが設定されている場合 (これは可能ですが、一般的ではありません)、どの DNS サーバもパーティション構造にコピーされず、以下で説明するメカニズムが適用されます。
- パーティション処理が無効になっているか、パーティションに DNS サーバが設定されていないか、解決する項目がパーティションに関連付けられていない場合、分割 DNS が提供する API によるリクエストごとに、使用する DNS サーバが選択されます。

分割 DNS サーバの追加

ドメイン固有 DNS サーバを追加し、そのサーバを所定のドメイン名に関連付けるには、以下の手順に従います。

ⓘ **重要:** 分割 DNS の最大エントリ数は 32 です。リストがいっぱいになった場合、新しいエントリは追加できません。

1. 「**ネットワーク > DNS**」に移動します。
2. IPv4/IPv6のタブで設定するIP バージョンを選択します。
3. 分割 DNS サーバのプロキシを有効にするには、「**分割 DNS サーバのプロシキを有効にする**」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す。
4. 「**分割 DNS**」タブに移動し「**追加**」を選択します。「**分割 DNS 登録の追加**」ダイアログが表示されます。
   「**DNS プロキシ**」を選択した場合は、そのためのページ「**DNS プロキシ**」も「**分割 DNS 登録の追加**」ダイアログ上に表示されます。
5. IP バージョンを選択します。
    - **IPv4**
    - **IPv6**
    - **両方**
6. 「**ドメイン名**」フィールドにドメイン名を入力します。この名前にはワイルドカード (*) を含めることができます (例:`*.SonicWall.com`)。
7. このドメインに対して 1 つ以上の IPv4/IPv6 分割 DNS サーバを設定するには、該当するフィールドに IP アドレスを入力します。

- **プライマリ サーバ (v4/v6)**
- **セカンダリ サーバ (v4/v6)** (オプション)
- **第 3 のサーバ (v4/v6)** (オプション)

8. 「**ローカル インターフェース**」リストからインターフェースを選択します。
9. 「**DNS プロキシ**」を有効にした場合は、以下の手順に従います。
    a. 「**持続時間**」を指定するには、「**DNS 応答の TTL 値を手動で設定する**」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。このオプションが選択されていない場合、TTL 値はDNS 応答の値と同じです。設定されている場合、TTL 値は設定値と同じです。
    ⓘ | **補足:** このオプションは、DNS プロキシで分割 DNS が使用される場合にのみ適用されます。
    b. キャッシュ エントリの最大持続時間を入力します。最小値は 1 秒、最大値は 9999999999999999 秒です。
10. 「**OK**」をクリックします。

ヒント: DNS サーバの設定時にどの IP バージョンを選択したかに関係なく、両方の IP バージョンの「**分割 DNS**」テーブルに DNS サーバが表示されます。

分割 DNS エントリの編集

分割 DNS エントリを編集するには、以下の手順に従います。

1. 「**ネットワーク > DNS**」に移動します。
2. 「**分割 DNS**」テーブルで、編集するエントリに関連付けられた「**編集**」アイコンを選択します。「**分割 DNS 登録の編集**」ダイアログが表示されます。
3. 変更を加えます。
4. 「**OK**」をクリックします。

分割 DNS エントリの削除

分割 DNS エントリを削除するには、以下の手順に従います。

1. 「**分割 DNS**」タブで、削除するエントリに関連付けられた「**削除**」アイコンを選択します。

2 つ以上の分割 DNS エントリを削除するには、以下の手順に従います。

1. 「**分割 DNS**」タブで、削除するエントリのチェックボックスを選択します。「**削除**」が使用可能になります。
2. 「**削除**」を選択します。

すべての分割 DNS エントリを削除するには、以下の手順に従います。

1. 「**すべて削除**」を選択します。

2

動的 DNS の設定

動的 DNS (DDNS) は、IP アドレスを動的に変更する際、DNS レコードを人の手を介さず自動的に更新できるようにするサービスで、様々な会社や組織によって提供されています。このサービスは、対象の IP アドレスが変更された場合にも、IP アドレスではなくドメイン名を使用することによって、ネットワーク アクセスを可能にします。

トピック:

動的 DNS について

動的 DNS (DDNS) は、IP アドレスを動的に変更する際、DNS レコードを人の手を介さず自動的に更新できるようにするサービスで、様々な会社や組織によって提供されています。このサービスは、対象の IP アドレスが変更された場合にも、IP アドレスではなくドメイン名を使用することによって、ネットワーク アクセスを可能にします。たとえば、ユーザが IP アドレスを ISP から動的に割り当てられるDSL 接続を使用している場合、DDNS を使用して IP アドレスを DDNS サーバに登録し、またその後のアドレス変更もすべて登録することによって、外部のホストは同じドメイン名を使いながら変更後のアドレスにアクセスを継続することができます。

動的 DNS の実装は、サービス プロバイダごとに内容が異なります。通信方式や登録できるレコードの種類、提供可能なサービスの種類に、厳密な標準はありません。また、プレミアム バージョンのサービスを有償で提供するプロバイダもあります。このため、特定の DDNS プロバイダをサポートするには、そのプロバイダ固有の実装との明示的な相互運用性が必要です。

プロバイダのほとんどは、IP アドレスの変更が発生した場合のみ DDNS レコードを更新するほうが望ましいと考えています。頻繁な更新は、特に登録 IP アドレスが変更されていない場合、プロバイダによってサービスの誤用と判断され、その結果 DDNS アカウントがロック アウトされる場合があります。プロバイダのページに掲載されている使用方針を確認し、その方針に準拠してください。SonicWall では DDNS プロバイダに関するテクニカル サポートは行いませんので、お問い合わせはプロバイダの方にお願いします。

動的 DNS は IPv4 と IPv6 の両方でサポートされています。

トピック:

サポートしている動的 DNS プロバイダ

すべてのプロバイダのすべてのサービスや機能をサポートしてはいません。また、サポートしているプロバイダのリストは、予告なく変更されることがあります。現在、SonicOS/X では、以下のプロバイダのサービスをサポートしています。

dns.org	SonicOS/X で DynDNS.org の DDNS を設定するには、ユーザ名、パスワード、メール エクスチェンジャー、バックアップ MX が必要です。
changeip.com	単一の古くからある動的 DNS サービスです。SonicOS/X の設定に必要なのは、ユーザ名、パスワード、ドメイン名のみです。
no-ip.com	SonicOS/X の設定に、ユーザ名、パスワード、ドメイン名のみを必要とする動的 DNSサービスです。ホスト名のグループ化もサポートしています。
Yi.org	SonicOS/X の設定に、ユーザ名、パスワード、ドメイン名のみを必要とする動的 DNSサービスです。動的更新を正しく行うには、`yi.org` 管理ページ上で RR レコードを作成する必要があります。

動的 DNS プロバイダによって提供される共通の追加サービスには次のようなものがあります。

ワイルドカード	サブドメインのワイルドカード参照を可能にします。例えば、yourdomain.dyndns.org を登録すると、サイトは *.yourdomain.dyndns.org (server.yourdomain.dyndns.org、www.yourdomain.dyndyn.org、ftp.yourdomain.dyndns.org など) からアクセスできるようになります。
メール エクスチェンジャー	SMTP サーバが DNS によってアドレスを検索してメールを送信できるように、ドメインの MX レコード エントリを作成します。 **補足:** 受信 SMTP が ISP によって遮断されることがよくあります。メールサーバをホストしようとする前にプロバイダへお問い合わせください。
バックアップ MX (dns.org、yi.org が提供)	プライマリ IP アドレスが停止中のときのために、MX レコード用のバックアップ IP アドレスを指定できます。
グループ	ホストをグループ化することによって、更新を個々のメンバーに対して複数回行うのではなく、グループ レベルで一度に実行できます。
オフライン IP アドレス	登録されたプライマリ IP アドレスがオフラインの場合、登録ホスト名用のバックアップ アドレスを指定できます。

DDNS プロファイルの設定に関する情報の参照先:「動的 DNS の設定」。

動的 DNS プロファイル

「**動的 DNS プロファイル**」テーブルは、設定された動的 DNS プロファイルに関する情報を提供します。

表示する IP バージョン	IPv4 および IPv6 動的 DNS プロファイル間でのテーブルの切り替えを可能にします。
プロファイル名	動的 DNS エントリを作成したときに割り当てた名前です。任意の値が可能で、識別のためにのみ使用されます。
ドメイン	動的 DNS エントリの完全修飾ドメイン名 (FQDN) です。

プロバイダ	このエントリが登録されている動的 DNS プロバイダです。
状況	最後にレポートされた時点または現在の動的 DNS エントリの状況です。

オンライン	動的 DNS エントリは、管理上オンラインです。このエントリの現在の IP 設定が、タイム スタンプとともに表示されます。
オフライン中	動的 DNS エントリは、管理上オフラインです。エントリが有効な場合、「**DDNS プロファイルの追加**」の「**詳細設定**」ページにある「**オフライン設定**」セクションで設定された動作を実行します。
誤用	動的 DNS プロバイダが、頻繁な更新を誤用であると見なしました。どのような場合に誤用とされるかを、動的 DNS プロバイダのガイドラインで確認してください。
IP 変更なし	誤用の可能性。IP アドレスを変更しない強制的な更新を行った場合、誤用であると見なす動的 DNS プロバイダがあります。自動更新は、アドレスや状況が変化した場合にのみ発生します。手動の更新や強制更新は、登録情報が間違っているなど、明確に必要な場合にのみ行われます。
無効	設定エラーまたはポリシー違反のため、アカウントを無効にされました。プロファイルの設定と、プロバイダの動的 DNS アカウント状況を確認してください。
無効なアカウント	提供されたアカウント情報が有効ではありません。プロファイルの設定と、プロバイダの動的 DNS アカウント状況を確認してください。
ネットワーク エラー	動的 DNS プロバイダと通信できません。ネットワーク エラーの疑いがあります。プロバイダがアクセス可能であり、オンラインになっていることを確認してください。時間を置いて再度実行してください。
プロバイダ エラー	動的 DNS プロバイダは、今回要求された動作を実行することができません。プロファイルの設定と、プロバイダの動的 DNS アカウント状況を確認してください。時間を置いて再度実行してください。
寄付者のアカウントではありません	プロバイダによって特定の機能 (オフライン アドレス設定など) が有料会員や寄付者にのみ利用可能な場合があります。どのサービスが有料または寄付が必要かの詳細は、プロバイダに確認してください。

有効	選択すると、このプロファイルが管理上有効になり、ネットワーク セキュリティ装置は、「**DDNS プロファイルの追加**」の「**詳細設定**」ページで設定した「**オンライン設定**」の動作を行います。この設定は、エントリの「**動的 DNS プロファイルの追加**」の「**この動的 DNS プロファイルを有効にする**」オプションを使用して制御することもできます。このオプションを非選択にするとプロファイルは無効になり、再度有効になるまで、このプロファイルのための動的 DNS プロバイダとの通信は発生しません。

オンライン	選択すると、このプロファイルは管理上オンラインになります。この設定は、エントリの「**動的 DNS プロファイルの追加**」で「**オンライン設定を使用する**」オプションを使用して制御することもできます。プロファイルが有効な間にこのオプションの選択を解除した場合、プロファイルはオフラインになり、ネットワーク セキュリティ装置は「**詳細設定**」ページで設定された「**オフライン設定**」の動作を行います。
構成	動的 DNS プロファイルを設定するための**編集**アイコンと、動的 DNS プロファイル登録を削除するための**削除**アイコンがあります。

トピック:

- 動的 DNS プロファイルの設定
- 動的 DNS プロファイルの編集
- 動的 DNS プロファイルの削除

動的 DNS プロファイルの設定

DDNS プロファイルの設定に関する一般的な情報の参照先:「動的 DNS の設定」。

動的 DNS サービスの使用は、利用する DDNS サービス プロバイダを選び、アカウントを設定することから始めます。同時に複数のプロバイダを利用することも可能です。「動的 DNS プロバイダ」に記載した各種プロバイダの一覧を参照してください。通常の登録手続きでは、プロバイダから確認の電子メールを受け取り、そのメールに埋め込まれている固有の URL へのアクセスを実行して最終確認を行います。選択したプロバイダのページにログインした後、管理用のリンク(一般に、「追加」や「管理」)を選択し、ホスト エントリを作成します。この作業は、SonicOS/X 上で動的 DNS クライアントを使用する前に行う必要があります。「**ネットワーク > 動的 DNS**」ページに、DDNS サービスを使用するように SonicWall ネットワーク セキュリティ装置を設定するための項目があります。

SonicWall セキュリティ装置で動的 DNS を設定するには、以下の手順に従います。

1. 「**ネットワーク > 動的 DNS**」に移動します。
2. 「**追加**」を選択します。「**動的 DNS プロファイルの追加**」ダイアログが表示されます。
3. 「**この動的 DNS プロファイルを有効にする**」がオンの場合は、このプロファイルは管理上有効になり、ネットワーク セキュリティ装置によって、「**詳細**」ページの「**オンライン設定**」セクションで定義されている動作が実行されます。このオプションは、既定では選択されています。
4. 「**オンライン設定を使用する**」チェックボックスがオンの場合は、このプロファイルの管理はオンラインになります。このオプションは、既定では選択されています。
5. 「**プロファイル名**」フィールドに、DDNS エントリに割り当てる名前を入力します。これには、「**動的DNS 設定**」テーブルでエントリを識別するのに使用する任意の名前を指定できます。名前は最小 1 文字、最大 63 文字です。
6. 「**プロバイダ**」で、動的 DNS プロバイダを選択します。これらのプロバイダに関する参照先: サポートしている動的 DNS プロバイダ。既定値は dyn.com です。

   ⓘ **重要:** 選択した DNS プロバイダで動的サービス レコードを作成しておく必要があります。

   ⓘ **ヒント:** どの DNS プロバイダでもすべてのオプションを使用できるわけではありません。また、ページ下部の「**補足**」には DNS プロバイダが HTTP または HTTPS プロトコルを使用しているかどうかや、そのプロバイダのウェブサイトへのリンクが表示されます。
7. 「**ユーザ名**」フィールドに、DNS プロバイダに持つアカウントのユーザ名を入力します。名前は最小 1 文字、最大 63 文字です。
8. 「**パスワード**」フィールドに DNS パスワードを入力します。名前は最小 1 文字、最大 31 文字です。

9. 「**ドメイン名**」フィールドに、DNS プロバイダに登録したホスト名の完全修飾ドメイン名 (FQDN) を入力します。ホスト名とドメインが、設定したものと同じであることを確認します。名前は最小 1 文字、最大 63 文字です。
10. オプションで、この動的 DNS プロファイルを特定の WAN インターフェースに割り当てるために、「**関連付け先**」から該当する WAN インターフェースを選択します。複数 WAN 負荷分散を設定している場合は、このオプションにより、予測可能な IP アドレスを動的 DNS サービスに通知できます。既定では、これは「**すべて**」に設定されていて、プロファイルがネットワーク セキュリティ装置上でどの WAN インターフェースでも自由に使用できることを意味します。
11. 「**プロバイダ**」で「dyn.com」を選択した場合は、ステップ 13 に進みます。
12. dyn.org を使用する際には、「**サービス種別**」で選択したサービスの種類に対応するサービス種別を選択します。

動的	無料の動的 DNS サービスです。このオプションは既定の設定です。
ユーザ定義	管理されたプライマリ DNS ソリューションで、プライマリおよびバックアップの統合 DNSサービスと、ウェブベースのインターフェースを提供します。動的、静的双方の IP アドレスをサポートしています。
静的	静的 IP アドレスを使用する無料の DNS サービスです。

13. 「**詳細**」を選択します。

ⓘ | **ヒント:** 一般に、このページの既定の設定をそのまま使用できます。

14. 「**オンライン設定**」セクションでは、動的 DNS プロバイダにどのアドレスを登録するかを指定します。次のどちらかを行います。

DDNS プロバイダに IP アドレスを検出させる	セキュリティ装置は DNS プロバイダによる IP アドレスの指定を許可します。 ⓘ | **補足:** IPv4 のみ。このオプションは、既定では選択されています。
自動的に IP アドレスをプライマリ WAN インターフェース IP アドレスに設定する	セキュリティ装置によって WAN IP アドレスが登録 IP アドレスとして割り付けられ、動的 DNS サーバによる自動検出に優先して使用されます。自動検出が適切に動作しない場合に役に立つ設定です。このオプションは、既定では選択されています。 ⓘ | **補足:** IPv6 の場合: このオプションは、既定では選択されています。
IP アドレスを手動で指定する	登録する IP アドレスを手動で指定および割り付けできます。

15. 「**オフライン設定**」セクションでは、ネットワーク セキュリティ装置で動的 DNS 登録がローカルにオフラインになっている (無効になっている) 場合に、動的 DNS サービス プロバイダにどの IP アドレスを登録するかを指定します。次のどちらかを行います。

何もしない	前に登録したアドレスを動的 DNS プロバイダでの現在のアドレスにすることができます。このオプションは、既定では選択されています。
プロバイダ サイトで事前に設定したオフライン IP アドレスを使用する	プロバイダでオフライン設定の手動設定をサポートしている場合は、このオプションを選択して、このプロファイルの管理がオフラインのときにこれらの設定を使用できます。
未知のホストにする	DDNS サービスの名前を非表示にします。
IP アドレスを手動で指定する	登録する IP アドレスを手動で指定および割り付けできます。

16. 「**OK**」をクリックします。

動的 DNS プロファイルの編集

DDNS プロファイルを編集するには、以下の手順に従います。

1. 「**ネットワーク > 動的 DNS**」に移動します。
2. 「**動的 DNS プロファイル**」テーブルで、該当するプロファイルの「**編集**」アイコンを選択します。「**DDNS プロファイルの編集**」ダイアログが表示されます。
3. 変更を加えます。各オプションの説明の参照先:「動的 DNS プロファイルの設定」。
4. 「**OK**」をクリックします。

動的 DNS プロファイルの削除

1 つまたはすべての動的 DNS プロファイルを削除できます。

DDNS プロファイルを削除するには、以下の手順に従います。

1. 「**ネットワーク > 動的 DNS**」に移動します。
2. 削除するプロファイルの**削除**アイコンを選択します。確認メッセージが表示されます。
3. 「**OK**」をクリックします。

すべての DDNS エントリを削除するには、以下の手順に従います。

1. 「**ネットワーク > 動的 DNS**」に移動します。
2. 削除するプロファイルを選択します。
3. 「**すべて削除**」を選択します。確認メッセージが表示されます。
4. 「**OK**」をクリックします。

3

DNS プロキシの設定

トピック:

DNS プロキシについて

IPv4 インターフェースは IPv4 インターネット上で名前解決を行うことができます。IPv6 インターフェースは、DNS プロキシを通じてのみ IPv6 インターネット上で名前解決を行うことができます。IPv4 と IPv6 が混在するネットワーク内の DNS サービスに IPv4 クライアントがアクセスできるように、SonicOS/X は DNS プロキシをサポートしています。

DNS プロキシ機能は、機器がクライアントに代わってホスト名解決要求をプロキシできる、トランスペアレントなメカニズムを提供します。このプロキシでは、既存の DNS キャッシュを使用できます。このキャッシュは、クエリに対して直接応答するように、管理者によって静的に設定されたものか、動的に学習されたもののどちらかです。

このプロキシは、特定の DNS サーバに対する DNS クエリのリダイレクトを、部分的なドメイン指定または完全なドメイン指定に従って選択的に行うことができます。これは、VPN トンネルまたは PPPoE 仮想リンクが複数のネットワーク接続を提供していて、一部の DNS クエリをあるネットワークに、その他のクエリを別のネットワークに誘導する必要がある場合に便利です。

DNS プロキシを利用している場合、LAN サブネットの機器は SonicWall ネットワーク セキュリティ装置を DNS サーバとして使用し、DNS クエリをこのネットワーク セキュリティ装置に送信します。ネットワーク セキュリティ装置は、DNS クエリを実際の DNS サーバにプロキシします。このように、ネットワーク セキュリティ装置は、ネットワークの DNS トラフィックにとって中心的な管理ポイントであり、ネットワークの DNS クエリを 1 か所で管理できるようにします。

ⓘ **補足:** セキュリティを維持するために、受信 DNS クエリのプロキシは、アクセス ルールと DPI によるチェック後にのみ行われます。

インターフェースで DNS プロキシを有効にすると、SonicOS/X によって 1 つの許可ルールが自動的に追加されます。

「**TCP 経由の 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。

トピック:

サポートされているインターフェース

DNS プロキシ機能は、以下の機器でサポートされています。

- 物理インターフェース
- VLAN インターフェース
- VLAN トランク インターフェース

各インターフェースのゾーンには、以下のみを使用できます。

- LAN
- DMZ
- WLAN

DNS サーバのライブネス検知とフェイルオーバー

複数の DNS サーバが設定されている場合に「最適」なサーバを決定するために、SonicOS/X は以下の要因を考慮します。

- DNS サーバの優先順位
- DNS サーバの状況（稼働中、休止中、不明）
- フェイルオーバー後の経過時間

DNS キャッシュ

DNS プロキシでは、よく使用されるドメインやホスト アドレスが DNS キャッシュ メモリに保存されます。DNS キャッシュ内のドメインに一致する DNS クエリを受け取ると、ファイアウォールは、DNS クエリや応答プロキシの処理を行わずに、キャッシュ レコードを使用してクライアントに直接応答を返します。

DNS キャッシュには次の 2 種類があります。

静的	管理者が手動で設定します。
動的	GMS によって自動学習されます。それぞれの DNS クエリについて、SonicOS/X DNS プロキシは、URI に対する精密検査を行い、有効な応答をキャッシュに記録します。

DNS クエリが既存のキャッシュ エントリに一致した場合、SonicOS/X DNS プロキシはキャッシュに記録されている URI を用いて直接応答を返します。これにより、通常はネットワーク トラフィックが減少し、結果としてネットワークの全体的なパフォーマンスが向上します。

静的 DNS キャッシュ サイズ

DNS キャッシュ エントリの固定サイズは、プラットフォームに関係なく、常に 256 です。静的 DNS キャッシュは、手動で削除しない限り、決して削除されません。

動的 DNS キャッシュ サイズ

動的 DNS キャッシュ サイズは、プラットフォームによって異なります。以下にその例を示します。

プラットフォーム	最大キャッシュ サイズ
SM 9400 SM 9600	4096
SM 9200	2048
NSA 4600 NSA 5600 NSA 6600	2048
NSA 2600 NSA 3600	1024
TZ600	512
TZ300/TZ300W TZ400/TZ400W TZ500/TZ500W	512

ネットワーク セキュリティ装置が DNS プロキシ キャッシュにエントリを追加しようとしたとき、キャッシュが最大サイズに達していた場合、ネットワーク セキュリティ装置は次の処理を行います。

1. 有効期限が最も近い DNS キャッシュ エントリを削除します。
2. 新しい DNS キャッシュ エントリを追加します。

DNS キャッシュの高可用性ステートフル同期

DNS プロキシは DNS キャッシュのステートフル同期をサポートしています。DNS キャッシュが追加、削除、または動的に更新された場合、DNS キャッシュはアイドル状態のファイアウォールとの同期をとります。

DHCP サーバ

インターフェース上で DNS プロキシが有効になっている場合、機器はそのインターフェース IP を DNS サーバ アドレスとしてクライアントにプッシュする必要があるので、DHCP サーバの設定は、「DNS/WINS」の「DHCP サーバ」設定でそのインターフェース アドレスを「DNS サーバ 1」のアドレスとして使用して、手動で行う必要があります。「**動的範囲の設定**」ダイアログの「**インターフェースの事前設定**」オプションを使用すると、この設定を簡単に行うことができます。選択したインターフェースで DNS プロキシが有効になっている場合、「DNS/WINS」ページに DNS サーバの IP が自動的に追加されます。DHCP サーバの設定方法に関する参照先: 「DNS の設定」。

ログの設定の有効化

DNS プロキシには複数のログが関連しています。これらのログは設定する必要があります。

パケットの監視

DNS プロキシのプロセスは、「**監視 > ツール & 監視 > パケット**」で監視できます。

DNS プロキシの設定

トピック:

DNS プロキシの有効化

DNS プロキシの有効化は、まず「**ネットワーク > DNS > DNS プロキシ**」ページで行ってから、各インターフェースに対して行う必要があります。これにより、異なるネットワーク セグメントに対してこの機能を個別に有効化する段階的な制御を実現できます。

DNS プロキシを有効にするには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**DNS プロキシを有効にする**」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。
3. 「**更新**」を選択します。
4. 「**ネットワーク > システム > インターフェース**」に移動します。
5. DNS プロキシを有効にする各インターフェースで、以下の手順を実行します。
    a. DNS プロキシを有効にするインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
    b. 「**詳細**」を選択します。
    c. 「**DNS プロキシを有効にする**」を選択します。このオプションは、DNS プロキシがグローバルで有効になっている場合にのみ表示されます。
    d. 「**OK**」をクリックします。
6. 「**適用**」を選択します。

DNS プロキシの設定

DNS プロキシを設定するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**DNS プロキシ モード**」リストで、ファイアウォールと DNS サーバとの間で DNS プロキシ パケットを送受信するための IP バージョンを選択します。
   - **IPv4 から IPv4**（既定）
   - **IPv4 から IPv6**
3. 「**DNS プロキシ プロトコル**」リストで、ファイアウォールと DNS サーバとの間で DNS プロキシ パケットを送受信するためのプロトコルを選択します。

   ⓘ **補足:** DNS プロキシ プロトコルは高度な機能です。この設定の詳細については、SonicWall テクニカル サポートにお問い合わせください。

   - **UDP と TCP**（既定値）
   - **UDP のみ**
4. 送信先に関係なく、すべての DNS プロキシ要求を許可するには、「**すべての DNS 要求に対して DNS プロキシを強制する**」を選択します。このオプションが無効になっている場合は、SonicWall ネットワーク セキュリティ装置宛ての DNS プロキシ要求のみが処理されます。このオプションは、既定では選択されていません。
5. UDP 経由の DNS 要求のみの場合は、「**DNS キャッシュを有効にする**」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。
6. 「**更新**」を選択します。

分割 DNS サーバの設定方法に関する参照先: 「分割 DNS 用のドメイン固有 DNS サーバの設定」。

静的 DNS キャッシュ エントリの表示と設定

ドメイン名	静的 DNA キャッシュ ドメインの名前。
IPv4 アドレス 1	静的 DNA キャッシュのプライマリ IPv4 アドレス。指定しない場合は、0.0.0.0。
IPv4 アドレス 2	静的 DNA キャッシュのセカンダリ IPv4 アドレス。指定しない場合は、0.0.0.0。
IPv6 アドレス 1	静的 DNA キャッシュのプライマリ IPv6 アドレス。指定しない場合は、::。
IPv6 アドレス 2	静的 DNA キャッシュのセカンダリ IPv6 アドレス。指定しない場合は、::。
構成	エントリごとに**編集**アイコンと**削除**アイコンがあります。

静的 DNS キャッシュ エントリを追加するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 「**追加**」を選択します。「**静的 DNS キャッシュの追加**」ダイアログが表示されます。

4. 追加する静的 DNS キャッシュ エントリごとに、以下の手順を実行します。
    a. 「**ドメイン名**」フィールドにドメイン名を入力します。
    b. IPv4 静的 DNS キャッシュの場合:
        1. 「**IPv4 アドレス 1**」フィールドにプライマリ IPv4 アドレスを入力します。
        2. 必要に応じて、「**IPv4 アドレス 2**」フィールドにセカンダリ IPv4 アドレスを入力します。
    c. IPv6 静的 DNS キャッシュの場合:
        1. 「**IPv6 アドレス 1**」フィールドにプライマリ IPv6 アドレスを入力します。
        2. 必要に応じて、「**IPv6 アドレス 2**」フィールドにセカンダリ IPv6 アドレスを入力します。
    d. 「**保存**」をクリックします。

静的 DNS キャッシュ エントリの削除

静的 DNS キャッシュ エントリを削除するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 削除する静的 DNS キャッシュ エントリを選択します。
4. そのエントリに関連付けられた「**削除**」アイコンをクリックします。

2 つ以上の静的 DNS エントリを削除するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 削除するエントリのチェックボックスをオンにします。「**削除**」が使用可能になります。
4. 「**構成**」列内の「**削除**」または「**削除**」アイコンをクリックします。

すべての静的 DNS エントリを削除するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 「**ドメイン名**」列の横にある最上部のチェックボックスをクリックします。すべてのエントリが選択されます。
4. 「**削除**」を選択します。

DNS キャッシュ オブジェクトの表示

表示する IP バージョン	IPv4 または IPv6 のどちらかを選択します。
ドメイン名	DNS サーバの名前
種別	動的または静的
IP アドレス	DNS サーバの IPv4 または IPv6 アドレス
持続時間	次のどちらかを行います • n 分 x 秒後に失効（動的 DNS） • 失効（動的 DNS）

	• 無期限（静的 DNS）
消去	各エントリの消去アイコン

動的 DNS キャッシュは DNS プロキシ処理時に自動的に追加されます。静的 DNS キャッシュは設定時に追加されます。動的 DNS キャッシュは TTL 値を持ち、消去が可能です。静的 DNS キャッシュは必ず削除する必要があります（参照先:「静的 DNS キャッシュ エントリの削除」）。

動的 DNS キャッシュ エントリの消去

動的 DNS キャッシュ エントリを消去するには、以下の手順に従います

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 消去するエントリを選択します。
4. そのエントリに関連付けられた「**消去**」アイコンをクリックします。

2 つ以上の動的 DNS エントリを消去するには、以下の手順に従います

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 削除するエントリのチェックボックスをオンにします。「**消去**」が使用可能になります。
4. 「**消去**」を選択します。

すべての動的 DNS キャッシュ エントリを消去するには、以下の手順に従います

1. 「**ネットワーク > DNS > DNS プロキシ**」に移動します。
2. 「**静的 DNS プロキシ キャッシュ登録**」タブをクリックします。
3. 「**DNS キャッシュの消去**」を選択します。

4

DNS セキュリティの設定

「**ネットワーク > DNS > DNS セキュリティ**」ページでは、ユニット レベルまたはグループ レベルで DNS セキュリティを手動で設定できます。

トピック:

DNS シンクホールについて

DNS シンクホールは、シンクホール サーバ、インターネット シンクホール、または Blackhole DNS とも呼ばれ、それに対応するドメイン名の使用を防ぐために偽情報を提供する DNS サーバです。DNS シンクホールは、悪意のあるトラフィックを検知して遮断するのに効果的であり、ボットやその他の望ましくないトラフィックからの防御に使用されます。

SonicOS/X では、シンクホールをブラック リストとホワイト リストで構成できます。

DNS セキュリティの設定を構成する

DNS セキュリティの設定を構成するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS セキュリティ**」に移動します。
2. 「**DNS シンクホール サービスを有効にする**」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。
3. 「動作」リストから、このサービスで実行する操作を選択します。
   - **ログだけを記録する**
   - **否定的な返信**
   - **偽装 IP による返信**: 表示可能になるフィールドに IPv4 アドレスと IPv6 アドレスを入力します。
4. 「**更新**」を選択します。
5. 「**ユーザ定義悪意のあるドメイン名**」タブを選択します。

6. 悪意のあるドメイン名として追加するドメイン名ごとに、以下の手順を実行します。
    a. 「**追加**」を選択します。「**ドメイン名を 1 つ追加する**」ダイアログが表示されます。
    b. 悪意のあるドメインの名前を「**ドメイン名**」フィールドに入力します。
    c. 「**保存**」をクリックします。
7. 「**ホワイト リスト**」タブを選択します。
8. ホワイト リストに追加するドメイン名ごとに、以下の手順を実行します。
    a. 「**追加**」を選択します。「**ドメイン名**」ダイアログが表示されます。
    b. 「**ドメイン名**」フィールドにホワイト リストのドメイン名を入力します。
    c. 「**保存**」をクリックします。
9. 「**更新**」を選択して変更を保存します。

リスト内のエントリの削除

リストからエントリを作成するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS セキュリティ**」に移動します。
2. 削除するエントリを選択するか、リスト内のすべての項目を選択する場合は「**ドメイン名**」列の横にあるチェックボックスを選択します。
3. 「**削除**」を選択します。

DNSトンネル検知の設定

DNS トンネリングとは、セキュリティ制御を迂回して標的の組織からデータを抜き取る手法です。DNS トンネルは、危険にさらされている内部ホスト用の完全なリモート制御チャンネルとして使用できます。オペレーティング システム (OS) のコマンド、ファイル転送、さらに IP トンネル全体などが抜き取られる可能性があります。

SonicOS/X は、DNS トンネリング攻撃を検知する機能を提供しており、不審なクライアントを表示したり、DNS トンネル検知用のホワイト リストを作成したりすることができます。

DNS トンネリング検知が有効になっている場合、不審な DNS パケットが破棄されるたびに SonicOS/X はそれをログに記録します。

ⓘ | **補足:** DNS トンネリング設定は、グループ レベルまたはユニット レベルで実行できます。

トピック:

- DNS トンネリング検知の設定
- 検知した不審なクライアントの表示
- DNS トンネル検知用ホワイト リストの作成
- DNS トンネル検知用ホワイト リストのエントリの削除

DNSトンネリング検知の設定

DNSトンネリング検知を設定するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS セキュリティ**」に移動します。
2. 「**DNS トンネル検知**」タブを選択します。
3. DNS トンネル検知を有効にするには、「**DNS トンネル検知を有効にする**」を選択します。
4. 検知されたすべてのクライアントからの DNS トラフィックを遮断するには、「**クライアントの DNS トラフィックをすべて遮断する**」を選択します。
5. 「**更新**」を選択します。

検知した不審なクライアントの表示

SonicOS/X は、「**検知した不審なクライアントの情報**」テーブルに DNS トンネルを確立したすべてのホストに関する情報を表示します。

検知した不審なクライアントを表示するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS セキュリティ**」に移動します。
2. 「**検知した不審なクライアントの情報**」タブを選択します。

このテーブルは、DNS トンネル検知が有効になっている場合にのみデータが入力されます。ホストは、クライアントの DNS トラフィックの遮断が有効になっている場合にのみ破棄されます。詳細に関する参照先: 「DNS トンネリング検知の設定」。

IP アドレス	不審なクライアントの IP アドレス。
MAC アドレス	不審なクライアントの MAC アドレス。
検知方法	不審なクライアントの検知に使用される DNS 種別: • **標準 DNS タイプ**: A、AAAA、CNAME • **特定 DNS 種別**: TXT、NULL、SRV、PRIVATE、MX など
インターフェース	DNS トンネルを確立するホストが検知されたインターフェース
遮断	ホストが遮断されたかどうかを示します

DNSトンネル検知用ホワイト リストの作成

安全と見なすことができる IP アドレスのホワイト リストを作成できます。検知された DNS トンネルの IP アドレスがホワイト リストのアドレスと一致する場合、DNS トンネル検知はバイパスされます。

DNS ホワイト リストを作成するには、以下の手順に従います。

1. 「**ネットワーク > DNS > DNS セキュリティ**」に移動します。
2. 「**DNS トンネル検知用ホワイト リスト**」タブを選択します。

3. ホワイトリストに追加するIPアドレスごとに、以下の手順を実行します。
    a. 「**追加**」を選択します。「**ホワイトリスト エントリを1つ追加する**」ダイアログが表示されます。
    b. 「**IPアドレス**」フィールドに、ホワイトリストに追加するドメインのIPアドレスを入力します。
    c. 「**保存**」をクリックします。
4. 「**適用**」をクリックします。

DNSトンネル検知用ホワイトリストのエントリの削除

DNSトンネル検知用ホワイトリストのすべてのエントリを削除するには、以下の手順に従います。

1. 「**ネットワーク**＞**DNS**＞**DNSセキュリティ**」に移動します。
2. 「**DNSトンネル検知用ホワイトリスト**」タブを選択します。
3. 削除するエントリを選択するか、リスト内のすべての項目を選択する場合は「**IPアドレス**」列の横にあるチェックボックスを選択します。
4. 「**削除**」を選択します。

5

SonicWall サポート

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

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

サポート ポータルでは、次のことができます。

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

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

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

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

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

SonicOS および SonicOSX ネットワーク DNS 管理ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005437-00 Rev B

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