接続、インストール、設定

この章で説明する内容は、次のとおりです。

- 接続、インストール、設定の概要 （1 ページ）
- 仮想アプライアンスの展開 （2 ページ）
- 操作モードの比較 （2 ページ）
- 接続、インストール、設定に関するタスクの概要 （8 ページ）
- アプライアンスの接続 （8 ページ）
- 設定情報の収集 （12 ページ）
- システム セットアップ ウィザード （14 ページ）
- アップストリーム プロキシ （23 ページ）
- ネットワーク インターフェイス （25 ページ）
- ハイ アベイラビリティを実現するためのフェールオーバー グループの設定 （41 ページ）
- Web プロキシ データに対する P2 データ インターフェイスの使用 （44 ページ）
- リダイレクト ホスト名とシステム ホスト名 （59 ページ）
- DNS の設定 （61 ページ）
- 接続、インストール、設定に関するトラブルシューティング （64 ページ）

接続、インストール、設定の概要

Web セキュリティアプライアンス では、次の動作モードを提供しています。

- 標準：Web セキュリティアプライアンス の標準動作モードには、オンサイトの Web プロキシサービスとレイヤ4トラフィックモニタリングが含まれます。これらのサービスはクラウド Web セキュリティコネクタモードでは使用できません。
- クラウド Web セキュリティコネクタ：クラウド Web セキュリティコネクタモードでは、アプライアンスは、Web セキュリティポリシーが適用されている Cisco Cloud Web Security（CWS）プロキシに接続してトラフィックをルーティングします。

アプライアンスには複数のポートが搭載されており、各ポートは割り当てられた1つ以上の特定のデータ型を管理します。

アプライアンスは、ネットワーク ルート、DNS、VLAN、およびその他の設定とサービスを使用して、ネットワーク接続とトラフィック代行受信を管理します。システムセットアップ ウィザードでは基本的なサービスと設定項目をセットアップでき、アプライアンスの Web インターフェイスでは設定の変更や追加オプションの設定ができます。

仮想アプライアンスの展開

仮想 Web セキュリティアプライアンス を展開するには、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

物理アプライアンスから仮想アプライアンスへの移行

物理アプライアンスから仮想アプライアンスに展開を移行するには、前のトピックで言及した『Virtual Appliance Installation Guide』、および使用している AsyncOS のバージョンに応じたリリース ノートを参照してください。

操作モードの比較

以下の表では、標準モードとクラウド コネクタ モードで使用可能なさまざまなメニュー コマンドを示し、それにより各モードで使用可能なさまざまな機能について説明します。

メニュー	標準モードで使用可能	クラウドコネクタ モードで使用可能
レポート	システム ステータス（System Status） 概要 Users ユーザ数（User Count） Web サイト（Web Sites） URL カテゴリ（URL Categories） アプリケーションの表示（Application Visibility） マルウェア対策（Anti-Malware） Advanced Malware Protection ファイル分析（File Analysis） AMP 判定の更新 クライアント マルウェア リスク（Client Malware Risk） Web レピュテーション フィルタ（Web Reputation Filters） レイヤ 4 トラフィック モニタ（Layer-4 Traffic Monitor） ユーザの場所別レポート（Reports by User Location） Web トラッキング（Web Tracking） システム容量（System Capacity） システム ステータス（System Status） スケジュール設定されたレポート（Scheduled Reports） アーカイブ レポート（Archived Reports）	システム ステータス（System Status）

メニュー	標準モードで使用可能	クラウドコネクタ モードで使用可能
Web セキュリティ マネージャ（Web Security Manager）	識別プロファイル（Identification Profiles） クラウド ルーティング ポリシー（Cloud Routing Policies） SaaS ポリシー 復号ポリシー（Decryption Policies） ルーティング ポリシー アクセス ポリシー 全体の帯域幅の制限（Overall Bandwidth Limits） Cisco データ セキュリティ 発信マルウェアスキャン（Outbound Malware Scanning） 外部データ消失防止 Web トラフィック タップ ポリシー SOCKS ポリシー（SOCKS Policies） カスタム URL カテゴリ 時間範囲およびクォータの定義（Define Time Ranges and Quotas） バイパス設定（Bypass Settings） レイヤ 4 トラフィック モニタ（Layer-4 Traffic Monitor）	識別プロファイル（Identification Profiles） クラウド ルーティング ポリシー（Cloud Routing Policies） 外部データ消失防止（External Data Loss Prevention） カスタム URL カテゴリ（Custom URL Categories）

メニュー	標準モードで使用可能	クラウドコネクタ モードで使用可能
セキュリティ サービス	Web プロキシ（Web Proxy） FTP プロキシ（FTP Proxy） HTTPS プロキシ（HTTPS Proxy） SOCKS プロキシ（SOCKS Proxy） PAC ファイル ホスティング（PAC File Hosting） 使用許可コントロール（Acceptable Use Controls） マルウェア対策とレピュテーション（Anti-Malware and Reputation） データ転送フィルタ（Data Transfer Filters） AnyConnect セキュア モビリティ（AnyConnect Secure Mobility） ユーザ通知（End-User Notification） L4 トラフィック モニタ（L4 Traffic Monitor） SensorBase レポート Cisco Cloudlock Cisco Cognitive Threat Analytics	Web プロキシ（Web Proxy）

メニュー	標準モードで使用可能	クラウドコネクタ モードで使用可能
ネットワーク（Network）	インターフェイス 透過リダイレクション（Transparent Redirection） ルート DNS 高可用性 内部 SMTP リレー（Internal SMTP Relay） 上位プロキシ（Upstream Proxy） 外部 DLP サーバ（External DLP Servers） Web トラフィック タップ（Web Traffic Tap） 証明書の管理（Certificate Management） 認証 SaaS のアイデンティティ プロバイダー Identity Services Engine	インターフェイス 透過リダイレクション（Transparent Redirection） ルート DNS 高可用性 内部 SMTP リレー（Internal SMTP Relay） 外部 DLP サーバ（External DLP Servers） 証明書の管理（Certificate Management） 認証 マシン ID サービス（Machine ID Service） クラウド コネクタ（Cloud Connector）

メニュー	標準モードで使用可能	クラウドコネクタ モードで使用可能
システム管理	ポリシー トレース（Policy Trace） アラート（Alerts） ログ サブスクリプション（Log Subscriptions） 返信先アドレス（Return Addresses） SSL の設定（SSL Configuration） Users Network Access タイム ゾーン 時刻設定（Time Settings） 設定の概要 設定ファイル（Configuration File） 機能キーの設定（Feature Key Settings） ライセンス キー（Feature Keys） アップグレードとアップデートの設定（Upgrade and Update Settings） システム アップグレード（System Upgrade） システム セットアップ ウィザード（System Setup Wizard） FIPS モード（FIPS Mode） 次の手順	アラート（Alerts） ログ サブスクリプション（Log Subscriptions） SSL の設定（SSL Configuration） Users Network Access タイム ゾーン 時刻設定（Time Settings） 設定の概要 設定ファイル（Configuration File） ライセンス キー（Feature Keys） アップグレードとアップデートの設定（Upgrade and Update Settings） システム アップグレード（System Upgrade） システム セットアップ ウィザード（System Setup Wizard）
Cisco CWS ポータル（Cisco CWS Portal）（ハイブリッド Web セキュリティ モードでのみ使用可能）	該当なし	該当なし

接続、インストール、設定に関するタスクの概要

タスク	詳細情報
• アプライアンスをインターネット トラフィックに接続する。	アプライアンスの接続 （8 ページ）
• 設定情報を収集して記録する。	設定情報の収集 （12 ページ）
• システム セットアップ ウィザードを実行する。	システム セットアップ ウィザード （14 ページ）
• HTTPS プロキシ設定、認証レルム、識別プロファイルを設定する。この手順はハイブリッド Web セキュリティ モードで実行する必要があります。	HTTPS プロキシのイネーブル化 認証レルム 識別プロファイルと認証
• （任意）アップストリーム プロキシを接続する。	アップストリーム プロキシ （23 ページ）

アプライアンスの接続

始める前に

- アプライアンスを設置するには、管理用アプライアンスにケーブルを配線して電源に接続し、そのアプライアンスのハードウェア ガイドの手順に従います。ご使用のモデルのマニュアルの場所については、ドキュメント セット を参照してください。
- 透過リダイレクションのためにアプライアンスを物理的に WCCP v2 ルータに接続する場合は、まず、WCCP ルータがレイヤ 2 リダイレクションに対応していることを確認します。
- 以下のシスコ推奨設定に注意してください。
  - パフォーマンスとセキュリティの向上のために、可能な場合はシンプレックス ケーブル（着信と発信トラフィック用の個別のケーブル）を使用します。

ステップ 1 管理インターフェイスを接続します（まだ接続していない場合）。

イーサネット ポート	注記
M1	接続可能な場所に M1 を接続します。 • 管理トラフィックを送受信します。 • （任意）Web プロキシ データ トラフィックを送受信します。 M1 にラップトップを直接接続して、アプライアンスを管理できます。 ホスト名（http://hostname:8080）を使用して管理インターフェイスに接続するには、アプライアンスのホスト名と IP アドレスを DNS サーバ データベースに追加します。
P1 および P2（任意）	• 発信方向の管理サービス トラフィックで使用可能ですが、管理には使用できません。 • [ポートM1は管理目的でのみ使用（Use M1 port for management only）]（[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページ）をイネーブルにします。 • データ インターフェイスを使用するように、サービスのルーティングを設定します。

ステップ 2 （任意）アプライアンスをデータ トラフィックに直接接続するか、透過リダイレクション デバイスを介して接続します。

イーサネットポート	明示的な転送	透過リダイレクション
P1/P2	P1 のみ： • [ポートM1は管理目的でのみ使用（Use M1 port for management only）] をイネーブルにします。 • P1 と M1 を異なるサブネットに接続します。 • 着信と発信の両方のトラフィックを受信できるように、デュプレックスケーブルを使用してP1を内部ネットワークとインターネットに接続します。 P1 および P2 • P1 をイネーブルにします。 • M1、P1、P2 を異なるサブネットに接続します。 • P2をインターネットに接続し、着信インターネットトラフィックを受信します。 システムセットアップウィザードの実行後、P2 をイネーブルにします。	デバイス：WCCP v2 ルータ： • レイヤ2リダイレクションの場合は、ルータを物理的に P1/P2 に接続します。 • レイヤ 3 リダイレクションの場合は、総称ルーティング カプセル化（GRE）でパフォーマンス上の問題が発生する可能性があるので注意してください。 • アプライアンス上に WCCP サービスを作成します。 デバイス：レイヤ 4 スイッチ： • レイヤ 2 リダイレクションの場合は、スイッチを物理的に P1/P2 に接続します。 • レイヤ 3 リダイレクションの場合は、総称ルーティング カプセル化（GRE）でパフォーマンス上の問題が発生する可能性があるので注意してください。 （注） アプライアンスはインラインモードをサポートしていません。
M1（任意）	[ポートM1は管理目的でのみ使用（Use M1 port for management only）] がディセーブルの場合は、M1 がデフォルトのデータ トラフィック用ポートになります。	該当なし

ステップ 3 （任意）レイヤ4トラフィックをモニタするには、プロキシポートの後ろと、クライアントIPアドレスのネットワーク アドレス変換（NAT）を実行するデバイスの前に、タップ、スイッチ、またはハブを接続します。

イーサネット ポート	注記
T1/T2	レイヤ4 トラフィックモニタのブロッキングを許可するには、Web セキュリティアプライアンス と同じネットワーク上にレイヤ 4 トラフィックモニタを配置します。 **推奨設定**： **デバイス：ネットワーク タップ**： • **ネットワーク タップに T1 を接続し、発信クライアント トラフィックを受信します。** • **ネットワーク タップに T2 を接続し、着信インターネット トラフィックを受信します。** その他のオプション： デバイス：ネットワーク タップ： • T1 でデュプレックス ケーブルを使用し、着信および発信トラフィックを受信します。 デバイス：スイッチ上のスパン化またはミラー化されたポート • 発信クライアント トラフィックを受信するように T1 を接続し、着信インターネット トラフィックを受信するように T2 を接続します。 • （準推奨）半二重または全二重ケーブルを使用して T1 を接続し、着信と発信の両方のトラフィックを受信します。 デバイス：ハブ： • （低推奨）デュプレックス ケーブルを使用して T1 を接続し、着信と発信の両方のトラフィックを受信します。 アプライアンスは、これらのインターフェイス上のすべての TCP ポートでトラフィックをリッスンします。

ステップ 4 外部プロキシをアプライアンスのアップストリームに接続し、外部プロキシがアプライアンスからデータを受信できるようにします。

次のタスク

設定情報の収集 （12 ページ）

関連項目

• ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）
• Web プロキシ データに対する P2 データ インターフェイスの使用 （44 ページ）

- WCCP サービスの追加と編集 （51 ページ）
- トランスペアレント リダイレクションの設定 （48 ページ）
- アップストリーム プロキシ （23 ページ）

設定情報の収集

以下のワークシートを使用して、システム セットアップ ウィザードの実行時に必要な設定値を記録できます。各プロパティの詳細については、システム セットアップ ウィザードの参照情報 （16 ページ）を参照してください。

システム セットアップ ウィザードのワークシート			
プロパティ	**値**	**プロパティ**	**値**
アプライアンスの詳細（Appliance Details）		**ルート**	
デフォルトの SystemHostname（Default SystemHostname）		**管理トラフィック（Management Traffic）**	
ローカル DNS サーバ（Local DNS Server(s)） **（インターネット ルートサーバを使用しない場合に必要）**		デフォルト ゲートウェイ （Default Gateway）	
DNS サーバ 1（DNS Server 1）		（任意）スタティック ルート テーブル名（Static Route Table Name）	
（任意）DNS サーバ 2（DNS Server 2）		（任意）スタティック ルートテーブルの宛先ネットワーク （Static Route Table Destination Network）	
（任意）DNS サーバ 3（DNS Server 2）		（任意）標準サービスのルータ アドレス（Standard Service Router Addresses）	

システム セットアップ ウィザードのワークシート			
プロパティ	値	プロパティ	値
（任意）時間の設定（**Time Settings**）		（任意）データ トラフィック（**Data Traffic**）	
ネットワーク タイム プロトコル サーバ（Network Time Protocol Server）		デフォルト ゲートウェイ（Default Gateway）	
（任意）外部プロキシの詳細（**External Proxy Details**）		スタティック ルート テーブル名（Static Route Table Name）	
プロキシ グループ名（Proxy Group Name）		スタティック ルート テーブルの宛先ネットワーク（Static Route Table Destination Network）	
プロキシサーバのアドレス（Proxy Server Address）		（任意）**WCCP** 設定（**WCCP Settings**）	
プロキシ ポート番号（Proxy Port Number）		WCCP ルータ アドレス（WCCP Router Address）	
インターフェイスの詳細（**Interface Details**）		WCCP ルータ パスフレーズ（WCCP Router Passphrase）	
管理（**M1**）ポート（**Management (M1) Port**）		管理設定（**Administrative Settings**）	
IPv4 アドレス（IPv4 Address）（必須） IPv6 アドレス（IPv6 Address）（任意）		管理者パスフレーズ（Administrator Passphrase）	

システム セットアップ ウィザードのワークシート			
プロパティ	**値**	**プロパティ**	**値**
ネットワーク マスク（Network Mask）		システム アラート メールの送信先（Email System Alerts To）	
ホストネーム		（任意）SMTP リレー ホスト（SMTP Relay Host）	
（任意）データ（P1）ポート（Data (P1) Port）			
IPv4（任意） IPv6 アドレス（IPv6 Address）（任意）			
ネットワーク マスク（Network Mask）			
ホストネーム			

システム セットアップ ウィザード

始める前に

- アプライアンスをネットワークとデバイスに接続します。アプライアンスの接続 （8 ページ）を参照してください。
- システム セットアップ ウィザードのワークシートを完成させます。設定情報の収集 （12 ページ）を参照してください。
- 仮想アプライアンスを設定する場合は、以下の手順に従います。
  - `loadlicense` コマンドを使用して、仮想アプライアンスのライセンスをロードします。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。
  - HTTP、および/または HTTPS インターフェイスを有効にします（コマンドライン インターフェイス（CLI）で、`interfaceconfig` コマンドを実行します）。

- システム セットアップ ウィザードで使用される各設定項目の参照情報は、システム セットアップ ウィザードの参照情報 （16 ページ）に記載されています。

警告 初めてアプライアンスをインストールする場合、または既存の設定を完全に上書きする場合にのみ、システム セットアップ ウィザードを使用してください。

ステップ 1 ブラウザを開き、Web セキュリティアプライアンス の IP アドレスを入力します。初めてシステム セットアップ ウィザードを実行するときは、以下のデフォルトの IP アドレスを使用します。

`https://192.168.42.42:8443`

または

`http://192.168.42.42:8080`

ここで、`192.168.42.42` はデフォルト IP アドレス、`8080` は HTTP のデフォルトの管理ポートの設定、`8443` は HTTPS のデフォルトの管理ポートです。

あるいは、アプライアンスが現在設定されている場合は、M1 ポートの IP アドレスを使用します。

ステップ 2 アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザー名とパスフレーズを入力します。デフォルトで、アプライアンスには以下のユーザー名とパスフレーズが付属します。

- ユーザー名：`admin`
- パスフレーズ：`ironport`

ステップ 3 パスフレーズをただちに変更する必要があります。

ステップ 4 [システム管理（System Administration）] > [システム セット アップウィザード（System Setup Wizard）] を選択します。

アプライアンスがすでに設定されている場合は、設定がリセットされるという警告が表示されます。システム セットアップ ウィザードを続行するには、[ネットワーク設定のリセット（Reset Network Settings）] をオンにしてから [構成のリセット（Reset Configuration）] ボタンをクリックします。アプライアンスがリセットされ、ブラウザが更新されてアプライアンスのホーム画面が表示されます。

ステップ 5 エンドユーザー ライセンス契約が表示されたら、内容を読んで同意します。

ステップ 6 続行するには、[セットアップの開始（Begin Setup）] をクリックします。

ステップ 7 必要に応じて、以下のセクションで提供されるリファレンス テーブルを使用して、すべての設定を行います。システム セットアップ ウィザードの参照情報 （16 ページ）を参照してください。

ステップ 8 設定情報を確認してください。オプションを変更する必要がある場合は、そのセクションで[編集（Edit）] をクリックします。

ステップ 9 [この設定をインストール（Install This Configuration）] をクリックします。

次のタスク

設定がインストールされると、[次のステップ（Next Steps）]ページが表示されます。ただし、セットアップ中に設定した IP、ホスト名、DNS 設定によっては、この段階でアプライアンスへの接続が失われることがあります。「ページが見つかりません（Page Not Found）」というメッセージがブラウザに表示される場合は、新しいアドレス設定が反映されるように URL を変更し、ページをリロードします。その後、実行する必要があるポスト セットアップ タスクを続行します。

システム セットアップ ウィザードの参照情報

- ネットワーク/システムの設定 （16 ページ）
- ネットワーク/ネットワーク インターフェイスおよび配線 （19 ページ）
- 管理およびデータ トラフィックのネットワーク/ルートの設定 （20 ページ）
- ネットワーク/透過的接続の設定 （20 ページ）
- ネットワーク/管理の設定 （21 ページ）

ネットワーク/システムの設定

プロパティ	説明
デフォルト システム ホスト名（Default System Hostname）	システム ホスト名は、以下の領域でアプライアンスの識別に使用される完全修飾ホスト名です。 • コマンドライン インターフェイス（CLI） • システム アラート • エンドユーザ通知ページおよび確認ページ • Web セキュリティアプライアンス が Active Directory ドメインに参加するときに、マシンの NetBIOS 名を作成する場合 システム ホスト名はインターフェイスのホスト名と直接対応しておらず、クライアントがアプライアンスに接続するために使用されません。

プロパティ	説明
DNS サーバ（DNS Server(s)）	• [インターネットのルートDNSサーバを使用（Use the Internet's Root DNS Servers）]：アプライアンスがネットワーク上の DNS サーバにアクセスできない場合に、ドメイン名サービス ルックアップにインターネットのルート DNS サーバを使用することを選択できます。 （注） インターネット ルート DNS サーバは、ローカル ホスト名を解決しません。アプライアンスでローカル ホスト名を解決する必要がある場合は、ローカルDNS サーバを使用して解決するか、CLIからローカルDNS に適切なスタティック エントリを追加する必要があります。 • [以下のDNSサーバを使用（Use these DNS Servers）]：アプライアンスがホスト名の解決に使用できるローカル DNS サーバにアドレスを提供します。 これらの設定の詳細については、DNS の設定 （61 ページ） を参照してください。
NTP サーバ（NTP Server）	システム クロックをネットワークまたはインターネット上の他のサーバと同期させるために使用する、Network Time Protocol（NTP）サーバ。 デフォルトは、time.sco.cisco.com です。
タイム ゾーン	アプライアンスの場所に応じたタイム ゾーン情報を提供します。メッセージヘッダーおよびログファイルのタイムスタンプに影響します。
アプライアンスの動作モード（Appliance Mode of Operation）	• 標準：標準的なオンプレミス ポリシーの適用に使用します。 • クラウド Web セキュリティ コネクタ：主に、Cisco クラウド Web セキュリティ サービスにトラフィックをダイレクトし、ポリシーを適用して脅威から防御するために使用します。 • ハイブリッド Web セキュリティ：クラウドとオンプレミス ポリシーの適用および脅威防御のために、Cisco クラウド Web セキュリティ サービスと併用されます。 これらの動作モードの詳細については、操作モードの比較 （2 ページ） を参照してください。

ネットワーク/ネットワーク コンテキスト

（注） 別のプロキシ サーバを含むネットワークでWeb セキュリティアプライアンス を使用する場合は、プロキシ サーバのダウンストリームで、クライアントのできるだけ近くに Web セキュリティアプライアンス を配置することを推奨します。

プロパティ	説明
ネットワークには他のWebプロキシがありますか?（Is there another web proxy on your network?）	ネットワークに以下のような別のプロキシがあるかどうか。 トラフィックがパススルーする必要のある他のプロキシがネットワークにありますか。この場合、Webセキュリティアプライアンスのアップストリームになりますか。 両方とも該当する場合は、チェックボックスをオンにします。これにより、1 つのアップストリーム プロキシのプロキシ グループを作成できます。後で、さらにアップストリームプロキシを追加できます。
プロキシ グループ名（Proxy group name）	アプライアンスでプロキシ グループの識別に使用される名前。
アドレス（Address）	アップストリーム プロキシ サーバーのホスト名または IP アドレス。
[ポート（Port）]	アップストリーム プロキシ サーバーのポート番号。

関連項目

- アップストリーム プロキシ （23 ページ）

ネットワーク/クラウド コネクタの設定

ページ名と設定を確認する必要があります。

設定	説明
クラウド Web セキュリティ プロキシ サーバー（Cloud Web Security Proxy Servers）	クラウド プロキシ サーバー（CPS）のアドレス（例：proxy1743.scansafe.net）。
失敗のハンドリング（Failure Handling）	AsyncOS がクラウド Web セキュリティ プロキシへの接続に失敗した場合、インターネットに [直接接続（Connect directly）] するか、[要求をドロップ（Drop requests）] します。

設定	説明
Cloud Web Security 認証スキーム（Cloud Web Security Authorization Scheme）	トランザクションを認証する方式： • Web セキュリティアプライアンス 公開 IPv4 アドレス。 • 各トランザクションに含まれている認証キー。Cisco Cloud Web Security Portal 内で認証キーを生成できます。

ネットワーク/ネットワーク インターフェイスおよび配線

Web セキュリティアプライアンス の管理および（デフォルトで）プロキシ（データ）トラフィック用に使用される IP アドレス、ネットワーク マスク、ホスト名。

アプライアンス管理インターフェイスに接続するときに（または、M1 がプロキシデータに使用される場合はブラウザ プロキシ設定で）、ここで指定したホスト名を使用できます。ただし、そのホスト名を組織の DNS に登録しておく必要があります。

設定	説明
イーサネット ポート（Ethernet Port）	（任意）データ トラフィック用に個別のポートを使用する場合は、[ポートM1は管理目的でのみ使用（Use M1 Port For Management Only）] をオンにします。 M1 インターフェイスを管理トラフィック専用として設定する場合は、データ トラフィック用の P1 インターフェイスを設定する必要があります。また、管理トラフィックとデータ トラフィック用に異なるルートを定義する必要があります。ただし、管理トラフィックとデータ トラフィックの両方を M1 インターフェイスとして使用する場合でも、P1 インターフェイスを設定できます。 システム セットアップ ウィザードでは、P1 ポートのみをイネーブルにして設定できます。P2 インターフェイスをイネーブルにする場合は、システム セットアップ ウィザードを終了してから行う必要があります。
IP アドレス/ネットマスク（IP Address / Netmask）	このネットワークインターフェイス上の Web セキュリティアプライアンス を管理する際に使用する IP アドレスとネットワークマスク。
ホストネーム	このネットワークインターフェイス上の Web セキュリティアプライアンス を管理する際に使用するホスト名。

ネットワーク/レイヤ 4 トラフィック モニターの配線

プロパティ	説明
レイヤ 4 トラフィック モニター（Layer-4 Traffic Monitor）	「T」インターフェイスに接続されている有線接続のタイプ： • **デュプレックス タップ。**T1 ポートは、着信と発信の両方のトラフィックを受信します。 • **シンプレックス タップ。**T1 ポートは（クライアントからインターネットへの）発信トラフィックを受信し、T2 ポートは（インターネットからクライアントへの）着信トラフィックを受信します。 シスコでは、パフォーマンスおよびセキュリティを向上させることができるため、可能な限りシンプレックスを使用することを推奨します。

管理およびデータ トラフィックのネットワーク/ルートの設定

（注） [ポートM1は管理目的でのみ使用（Use M1 port for management only）] をイネーブルにした場合、このセクションには、管理トラフィックとデータ トラフィック用の個別のセクションが表示されます。それ以外の場合は 1 つの結合されたセクションが表示されます。

プロパティ	説明
デフォルト ゲートウェイ（Default Gateway）	管理およびデータ インターフェイスを通過するトラフィックに使用するデフォルト ゲートウェイの IP アドレス。
スタティック ルート テーブル（Static Routes Table）	管理およびデータ トラフィック用のオプションのスタティック ルート。複数のルートを追加できます。 • **名前（Name）**：スタティック ルートの識別に使用する名前。 • **内部ネットワーク（Internal Network）**：このルートのネットワーク上の宛先の IPv4 アドレス。 • **内部ゲートウェイ（Internal Gateway）**：このルートのゲートウェイ IPv4 アドレス。ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。

ネットワーク/透過的接続の設定

（注） デフォルトでは、クラウドコネクタはトランスペアレントモードで展開され、レイヤ4スイッチまたは WCCP バージョン 2 ルータと接続する必要があります。

プロパティ	説明
レイヤ4スイッチまたはデバイスなし（Layer-4 Switch or No Device）	Web セキュリティアプライアンス が透過リダイレクション用にレイヤ 4 スイッチに接続されていること、または透過リダイレクション デバイスを使用せず、クライアントがアプライアンスに明示的に要求を転送することを指定します。
WCCP v2 ルータ（WCCP v2 Router）	Web セキュリティアプライアンス が WCCP バージョン 2 対応ルータに接続されていることを指定します。 WCCP バージョン 2 ルータに接続する場合、少なくとも 1 つの WCCP サービスを作成する必要があります。この画面で、またはシステム セットアップ ウィザードの終了後に、標準サービスをイネーブルにでき、複数のダイナミック サービスを作成することもできます。 標準サービスをイネーブルにすると、ルータ セキュリティをイネーブルにして、パスフレーズを入力することもできます。ここで使用されるパスフレーズは、同じサービス グループ内のすべてのアプライアンスと WCCP ルータで使用する必要があります。 標準サービス タイプ（別名「Web キャッシュ」サービス）には、固定 ID「ゼロ」、固定リダイレクト方式「宛先ポート別」、固定宛先ポート「80」 が割り当てられます。 ダイナミック サービス タイプでは、カスタム ID、ポート番号、およびリダイレクト オプションとロード バランシング オプションを定義できます。

ネットワーク/管理の設定

プロパティ	説明
管理者パスフレーズ（Administrator Passphrase）	管理のためにWeb セキュリティアプライアンス にアクセスするときに使用されるパスフレーズ。
システム アラート メールの送信先（Email System Alerts To）	アプライアンスがシステム アラートを送信する宛先の電子メール アドレス。
SMTP リレーホスト経由で電子メールを送信（Send Email via SMTP Relay Host）（任意）	AsyncOS がシステムで生成された電子メール メッセージの送信に使用できる、SMTP リレー ホストのアドレスとポート。 SMTP リレーホストが定義されていない場合、AsyncOS は MX レコードにリストされているメール サーバを使用します。
オートサポート（AutoSupport）	アプライアンスがシステム アラートと毎週のステータス レポートをシスコ カスタマー サポートに送信するかどうかを指定します。

プロパティ	説明
SensorBase ネットワークに参加（SensorBase Network Participation）	Cisco SensorBase ネットワークに参加するかどうかを指定します。参加する場合、制限付き参加または標準（完全な）参加を設定できます。デフォルトは標準です。 SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネット トラフィックのグローバルな監視リストを保持する脅威管理データベースです。SensorBase ネットワーク参加をイネーブルにすると、Web セキュリティアプライアンス は SensorBase ネットワーク データの価値を高めるために、HTTP 要求に関する匿名の統計情報をシスコに送信します。

セキュリティ/セキュリティ設定

オプション	説明
グローバルポリシーのデフォルトアクション（Global Policy Default Action）	システム セットアップ ウィザードの完了後、デフォルトで、すべての Web トラフィックをブロックするか、モニターするかを選択します。グローバル アクセス ポリシーのプロトコルとユーザー エージェントの設定を編集することで、後でこの動作を変更できます。デフォルトの設定は、トラフィックのモニターです。
L4 トラフィック モニター（L4 Traffic Monitor）	システム セットアップ ウィザードの完了後、デフォルトで、レイヤ 4 トラフィック モニターでモニターするか、疑わしいマルウェアをブロックするかを選択します。この設定は後で変更できます。デフォルトの設定は、トラフィックのモニターです。
使用許可コントロール（Acceptable Use Controls）	[使用許可コントロール（Acceptable Use Controls）] をイネーブルにするかどうかを指定します。 イネーブルにすると、使用許可コントロールにより、URL フィルタリングに基づいてポリシーを設定できます。また、アプリケーションの可視性と制御に加えて、セーフ サーチの適用などの関連オプションを使用できるようになります。デフォルトの設定はイネーブルです。
評価フィルタリング（Reputation Filtering）	グローバル ポリシー グループに対して Web レピュテーション フィルタリングをイネーブルにするかどうかを指定します。 Web 評価フィルタは、Web サーバーの動作を分析し、評価スコアを URL に割り当て、URL ベースのマルウェアを含む可能性を判定するセキュリティ機能です。デフォルトの設定はイネーブルです。

オプション	説明
マルウェアとスパイウェアのスキャン（Malware and Spyware Scanning）	Webroot、McAfee、またはSophosによるマルウェアやスパイウェアのスキャンをイネーブルにするかどうかを指定します。デフォルトの設定では、3 つのオプションがすべて有効になります。クラウド ポリシーで通常使用可能なサービスに対応して、ほとんどのセキュリティ サービスは自動的に有効/無効になります。同様に、ポリシー関連のデフォルトは適用されません。少なくとも 1 つのスキャン オプションをイネーブルにする必要があります。 オプションをイネーブルにした場合は、検出されたマルウェアをモニターするかブロックするかも選択します。デフォルトの設定は、マルウェアのモニターです。 システム セットアップ ウィザードを完了後、マルウェア スキャンを追加設定することもできます。
Cisco データ セキュリティ フィルタリング（Cisco Data Security Filtering）	Ciscoデータ セキュリティ フィルタをイネーブルにするかどうかを指定します。 イネーブルにすると、Cisco データ セキュリティ フィルタはネットワークから発信されるデータを評価し、ユーザーは、特定タイプのアップロード要求をブロックするシスコ データ セキュリティ ポリシーを作成できます。デフォルトの設定はイネーブルです。

アップストリーム プロキシ

Web プロキシは、Web トラフィックを宛先 Web サーバに直接転送することも、ルーティング ポリシーを使用して外部アップストリーム プロキシにリダイレクトすることもできます。

- アップストリーム プロキシのタスクの概要 （23 ページ）
- アップストリーム プロキシのプロキシ グループの作成 （24 ページ）

アップストリーム プロキシのタスクの概要

タスク	詳細情報
• Cisco Web セキュリティアプライアンス のアップストリームに外部プロキシに接続する。	アプライアンスの接続 （8 ページ）。
• アップストリームプロキシのプロキシグループを作成して設定する。	アップストリーム プロキシのプロキシ グループの作成 （24 ページ）。
• プロキシグループのルーティングポリシーを作成し、アップストリーム プロキシにルーティングするトラフィックを管理する。	インターネット要求を制御するポリシーの作成

アップストリーム プロキシのプロキシ グループの作成

ステップ 1 [ネットワーク（Network）] > [アップストリームプロキシ（Upstream Proxies）] を選択します。

ステップ 2 [グループの追加（Add Group）] をクリックします。

ステップ 3 プロキシ グループの設定を完了させます。

プロパティ	説明
Name	ルーティング ポリシーなどでアプライアンス上のプロキシ グループの識別に使用される名前など。
プロキシ サーバ（Proxy Servers）	グループのプロキシ サーバのアドレス、ポート、再接続試行（プロキシが応答しない場合）。必要に応じて、各プロキシ サーバの行を追加または削除できます。 （注） 同じプロキシサーバを複数回追加して、プロキシグループのプロキシ間に不均衡に負荷を分散できます。
ロード バランシング（Load Balancing）	複数のアップストリーム プロキシ間のロードバランス要求のために Web プロキシが使用する方法。次から選択します。 • [なし（フェールオーバー）（None (failover)）]。Web プロキシは、グループ内の 1 つの外部プロキシにトランザクションを送信します。一覧表示されている順序でプロキシへの接続を試みます。あるプロキシに到達できない場合、Web プロキシはリストの以下のプロキシに接続を試みます。 • [最少接続（Fewest connections）]。Web プロキシは、グループ内のざまざまなプロキシにおけるアクティブな要求の数を追跡し、その時点で接続数が最も少ないプロキシにトランザクションを送信します。 • **[ハッシュベース（Hash based）]。**[最も長い間使われていない（Least recently used）]。すべてのプロキシがアクティブである場合、Web プロキシは、最も長い間トランザクションを受信していないプロキシにトランザクションを送信します。この設定はラウンドロビンに似ています。異なる点は、Web プロキシが、異なるプロキシ グループのメンバーであるプロキシが受信したトランザクションも考慮するということです。つまり、あるプロキシが複数のプロキシグループのリストに含まれている場合でも、[最も長い間使われていない（least recently used）] オプションによってそのプロキシが過負荷になることはほとんどありません。 • [ラウンドロビン（Round robin）]。Web プロキシは、リストに記載されている順序で、グループ内のすべてのプロキシにトランザクションを均等に割り当てます。 （注） 複数のプロキシを定義するまで、[ロードバランシング（Load Balancing）] オプションはグレー表示されます。

プロパティ	説明
失敗のハンドリング（Failure Handling）	このグループのすべてのプロキシが失敗した場合のデフォルト アクションを指定します。次から選択します。 • **[直接接続（Connect directly）]**。宛先サーバに直接、要求を送信します。 • **[要求をドロップ（Drop requests）]**。要求を転送しないで、廃棄します。

ステップ 4 変更を送信し、保存します。

次のタスク

- ポリシーの作成

ネットワーク インターフェイス

- IP アドレスのバージョン （25 ページ）
- ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）

IP アドレスのバージョン

標準モードでは、Cisco Web セキュリティアプライアンス は大部分の場合に IPv4 と IPv6 アドレスをサポートします。

（注） クラウドコネクタモードでは、Web セキュリティアプライアンス は IPv4 のみをサポートします。

DNS サーバは、IPv4 と IPv6 の両方のアドレスと共に結果を返すことができます。DNS の設定項目には [IP アドレスバージョン設定（IP Address Version Preference）] が含まれているので、以下の場合における AsyncOS の動作を設定できます。

インターフェイス/サービス	IPv4	IPv6	注記
M1 インターフェイス	必須	オプション	IPv6 アドレスを使用するには、デフォルトの IPv6 ゲートウェイを定義する IPv6 ルーティング テーブルが必要です。ネットワークによっては、ルーティング テーブルで IPv6 スタティック ルートも指定する必要があります。

インターフェイス/サービス	IPv4	IPv6	注記
P1 インターフェイス	オプション	オプション	P1 インターフェイスに IPv6 アドレスが設定されており、アプライアンスが分割ルーティング（個別の管理ルートとデータルート）を使用している場合、P1 インターフェイスは管理ルート上に設定された IPv6 ゲートウェイを使用できません。代わりに、データ ルーティング テーブルに IPv6 ゲートウェイを指定します。
P2 インターフェイス	オプション	オプション	—
データ サービス	サポート対象	サポート対象	—
制御および管理サービス	サポート対象	一部サポートあり	イメージ（エンドユーザ通知ページのカスタム ロゴなど）には IPv4 が必要です。
AnyConnect セキュア モビリティ（MUS）	サポート対象	サポート対象外	—

関連項目

- ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）
- DNS の設定 （61 ページ）

ネットワーク インターフェイスのイネーブル化または変更

- インターフェイス IP アドレスの追加または変更
- レイヤ 4 トラフィック モニタの配線タイプの変更
- 管理およびデータ トラフィックの分割ルーティングのイネーブル化

ステップ 1 [ネットワーク（Network）] > [インターフェイス（Interfaces）] を選択します。
ステップ 2 [設定の編集（Edit Settings）] をクリックします。
ステップ 3 インターフェイスのオプションを設定します。

オプション	説明
インターフェイス	M1、P1、または P2 インターフェイスの新しい IPv4 または IPv6 アドレス、ネットマスク、ホスト名の詳細を追加するか、既存の詳細を変更します。 • **M1**：AsyncOS には M1（管理）ポートの IPv4 アドレスが必要です。IPv4 アドレスに加えて、IPv6アドレスも指定できます。デフォルトで、管理インターフェイスはアプライアンスおよび Web プロキシ（データ）のモニタリングを管理するために使用されます。ただし、管理用途専用の M1 ポートを設定できます。 • **P1** および **P2**：データ ポートの IPv4 アドレス、IPv6 アドレス、または両方を使用します。データ インターフェイスは Web プロキシによるモニタリングとレイヤ 4 トラフィック モニタによるブロッキング（任意）で使用されます。これらのインターフェイスを設定して、DNS、ソフトウェアアップグレード、NTP、および traceroute データ トラフィックなどの発信サービスをサポートすることもできます。 （注） 管理およびデータ インターフェイスをすべて設定する場合、それぞれに異なるサブネット上の IP アドレスを割り当てる必要があります。 （注） 分割ルーティングが有効になっている場合、管理インターフェイスはスマートライセンスポータルと通信できません。Web セキュリティアプライアンスをスマートライセンスポータルに登録するには、データインターフェイスを選択します。 （注） 分割ルーティングが設定されている場合、Web セキュリティアプライアンス はデータインターフェイスを使用して外部 DLP サーバーに接続し、管理インターフェイスは管理トラフィックのみに制限されます。これにより、トラフィックを DLP サーバーにルーティングする間、すべての DLP トラフィックが管理トラフィックではなくデータトラフィックと見なされます。 たとえば、DLP アドレスでフィルタリングされる P1 インターフェイスと M1 インターフェイスを持つ 2 つのパケットキャプチャがある場合、DLP トラフィックは両方のインターフェイスで検出されます。これは、キープアライブパケットを DLP サーバーに送信する管理インターフェイスと、データインターフェイスからの DLP トラフィックによるものです。
管理サービス用の分離ルーティング（Separate Routing for Management Services）	M1 を管理トラフィック専用に制限して、データ トラフィック用に別のポートを使用する必要がある場合は、[M1ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] をオンにします。 （注） M1 を管理トラフィック専用にする場合は、別のサブネットにプロキシ トラフィック用のデータインターフェイスを少なくとも 1 つ設定します。管理トラフィックとデータ トラフィック用に異なるルートを定義してください。

オプション	説明
アプライアンス管理サービス（Appliance Management Services）	以下のネットワーク プロトコルの使用をイネーブルまたはディセーブルにして、そのデフォルトのポート番号を指定します。 • **FTP**：デフォルトでディセーブルになります。 • **SSH** • **HTTP** • **HTTPS** また、HTTP トラフィックの HTTPS へのリダイレクションをイネーブルまたはディセーブルにできます。

ステップ 4 変更を送信し、保存します。

次のタスク

IPv6 アドレスを追加する場合は、IPv6 ルーティング テーブルを追加します。

関連項目

- アプライアンスの接続 （8 ページ）。
- IP アドレスのバージョン （25 ページ）
- TCP/IP トラフィック ルートの設定 （45 ページ）

ネットワーク インターフェイス カードの設定

この章で説明する内容は、次のとおりです。

- イーサネット インターフェイスのメディア設定 （28 ページ）
- ネットワーク インターフェイス カードのペアリングおよびチーミング （29 ページ）
- etherconfig コマンドを使った NIC ペアリングのイネーブル化 （30 ページ）
- NIC ペアリングを設定するためのガイドライン （37 ページ）

イーサネット インターフェイスのメディア設定

etherconfig コマンドを使用して、イーサネット インターフェイスのメディア設定にアクセスできます。個々のイーサネットインターフェイスが現在の設定と共に一覧表示されます。インターフェイスを選択すると、適切なメディア設定が表示されます。

etherconfig を使ったイーサネット インターフェイスのメディア設定の編集

etherconfig コマンドを使って、イーサネット インターフェイスのデュプレックス設定（全二重/半二重）や速度（10/100/1000 Mbps）を設定できます。デフォルトでは、インターフェイスはメディア設定を自動的に選択します。これはオーバーライドできます。

（注） 「接続、インストール、設定」のトピックの説明に従ってGUIのシステム設定ウィザード（またはコマンドライン インターフェイスの **systemsetup** コマンド）を実行し、変更を確定していれば、アプライアンス上でデフォルトのイーサネットインターフェイス設定が構成されているはずです。

メディア設定の編集例

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
[]> MEDIA
Ethernet interfaces:
1. Management (Autoselect: <1000baseT full-duplex>) 00:50:56:87:a6:46
2. P1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
3. P2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:6a:42
4. T1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
5. T2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:fc:01

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

ネットワーク インターフェイス カードのペアリングおよびチーミング

NIC ペアリングで 2 つの物理データポートを組み合わせることにより、NIC からアップストリームのイーサネットポートへのデータパスに障害が発生した場合に、バックアップ イーサネットインターフェイスを提供できます。ペアリングでは、基本的に各イーサネットインターフェイスをプライマリ インターフェイスおよびバックアップ インターフェイスとして設定します。プライマリインターフェイスに障害が発生した場合（NIC とアップストリームノード間のキャリアが途切れた場合など）は、バックアップインターフェイスがアクティブになり、アラートが送信されます。プライマリインターフェイスが有効になると、このインターフェイスがアクティブになります。この製品のマニュアルでは、「NIC ペアリング」と「NIC チーミング」は同義語です。

（注） NIC ペアリングは、S170、S190、および S195 Web ゲートウェイでは使用できません。

十分な数のデータポートがあれば、複数のNICペアを作成できます。ペアを作成するときは、任意のデータ ポートを組み合わせることができます。次に例を示します。

- Data 1 と Data 2

- Data 3 と Data 4
- Data 2 と Data 3

一部の Web ゲートウェイは、光ファイバ ネットワーク インターフェイス オプションを備えています。その場合は、各 Web ゲートウェイ上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス（Data 3 と Data 4）が表示されます。異種混在構成では、これらのギガビット光ファイバインターフェイスは、銅線（Data 1、Data 2、および Management）インターフェイスとペアにすることができます。

Web セキュリティアプライアンス は、NIC ペアリングインターフェイスのパケットキャプチャをサポートしていません。パケットキャプチャは、アクティブなインターフェイスにのみ適用されます。たとえば、P1 と P2 の両方がペアになっている場合、P1 と P2 のどちらもユーザー インターフェイスまたは CLI で設定されません。

NIC ペアリングと VLAN

VLAN（「VLAN の使用によるインターフェイス能力の向上」を参照）は、プライマリインターフェイスでのみ許可されます。

NIC ペアの名前

NIC ペアを作成するときは、ペアの名前を指定する必要があります。バージョン 4.5 よりも前の AsyncOS で作成した NIC ペアには、アップグレード後、自動的に「Pair 1」というデフォルト名が指定されます。

NIC ペアリングで生成されたアラートは、特定の NIC ペアをその名前で参照します。

NIC ペアリングと既存のリスナー

リスナーが割り当てられたインターフェイスで NIC ペアリングをイネーブルにすると、バックアップインターフェイスに割り当てられた全リスナーの削除、再割り当て、ディセーブル化のいずれかを選択するように求められます。

etherconfig コマンドを使った NIC ペアリングのイネーブル化

（注） NIC ペアリングは、S170、S190、および S195 Web ゲートウェイでは使用できません。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
Choose the operation you want to perform:
- NEW - Create a new pairing.
[]> NEW
Please enter a name for this pair (Ex: "Pair 1"):
[]> DP1
```

```
1. P1
2. P2
Enter the name or number of the primary ethernet interface you wish bind to.
[]> 1

1. P2
2. T1
3. T2
Enter the name or number of the backup ethernet interface you wish to pair.
[]> 2

Paired interfaces:
1. DP1:
        Primary (P1)
        Backup (T1)

Choose the operation you want to perform:
- NEW - Create a new pairing.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:40:34 2020 MST
example.com> interfaceconfig


Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> NEW
Ethernet interface:
1. Management
2. DP1
3. P2
[1]> 2
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[]> 10.10.102.66
Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 27
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Hostname:
[]> example.com
```

```
Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
2. P1 (10.10.102.66/27 on DP1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
example.com>example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:43:18 2020 MST
example.com> exitexample.com:rtestuser 53] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:fc:01
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

```
        groups: lo
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet6 fe80::250:56ff:fe87:a646%lagg0 prefixlen 64 scopeid 0x7
        inet 10.10.102.66 netmask 0xfffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        groups: lagg
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
example.com:rtestuser 54]
```

P1 インターフェイスの停止

P1 と T1 はペアになっており、DP1 と名付けられています。P1 が停止すると、T1 がアクティブになります。次の例では、lagg0 インターフェイスを参照します。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
1. DP1:
        Backup (T1) Standby, Link is up
        Primary (P1) Active, Link is up
2. DP2:
        Backup (T2) Standby, Link is up
        Primary (P2) Active, Link is up

Choose the operation you want to perform:
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com>
example.com> exit

example.com:rtestuser 115] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
```

```
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 116]
example.com:rtestuser 116] ifconfig nic1 down
example.com:rtestuser 117] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
```

```
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=1<MASTER>
        laggport: nic3 flags=4<ACTIVE>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffffe0 broadcast 10.10.166.95
```

```
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 118]
```

P1 インターフェイスの起動

```
example.com:rtestuser 118] ifconfig nic1 up
example.com:rtestuser 119] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
```

```
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 120]
example.com:rtestuser 120]
```

NIC ペアリングを設定するためのガイドライン

M2、Data 1、Data 2 は、プライマリまたはセカンダリとして使用したり、IP アドレスで設定したりできません。

表 *1:*

ポート	IP アドレスとして設定	操作	対処方法	分割ルーティング有効	
				プライマリ（Primary）	セカンダリ（Secondary）
P1（プロキシ）	対応	有効	着信と発信の両方に対応するネットワークにP1を接続します 。		P2、T1、T2

ポート	IP アドレスとして設定	操作	対処方法	分割ルーティング有効	
				プライマリ（Primary）	セカンダリ（Secondary）
				P1 を NIC ペアリングのプライマリとして選択できます （注） P2 をプライマリとして選択した場合は、P1 の IP アドレスを削除する必要があります。	

ポート	IP アドレスとして設定	操作	対処方法	分割ルーティング有効	
				プライマリ（Primary）	セカンダリ（Secondary）
P1 + P2（プロキシ）	対応	有効	P1 を内部ネットワークに接続し、 P2 をインターネットに接続します。	P2 をプライマリとして、P1 をセカンダリとして選択した場合は、P1 の IP アドレスを削除する必要があります。 NIC ペアリング中に、IP を削除するように求められます。	T1、T2
T1（トラフィックモニタリング）	非対応	デュプレックスタップ	1 本のケーブルですべての着信および発信トラフィックに対応します。	NA	NA
T1 + T2（トラフィックモニタリング）	対応	シンプルタップ	1 本のケーブルでインターネットに宛てたすべてのパケットに対応し（T1）、もう 1 本のケーブルでインターネットから着信するすべてのパケットに対応します（T2）。	NA	NA

（注） P1 の IP を削除することを選択した場合、P1 は分割ルーティングで設定されません。P2 または作成された NIC ペアに IP アドレスが割り当てられると、P2 のみが設定された状態で分割ルーティングが有効になります。リンクアグリゲーション（LAGG）インターフェイスは、IP アドレスがプライマリ（P2）または NIC ペアに割り当てられない限り表示されません。プライマリ（P2）または NIC ペアに IP アドレスが割り当てられると、LAGG インターフェイスが作成されます。

ハイ アベイラビリティを実現するためのフェールオーバー グループの設定

共通アドレス冗長プロトコル（CARP）を使用すると、Web セキュリティアプライアンス ではネットワーク上の複数のホストで IP アドレスを共有できるようになります。これにより IP 冗長性が実現され、それらのホストから提供されるサービスのハイアベイラビリティを確保できます。

フェールオーバーはプロキシ サービスでのみ使用できます。フェールオーバー グループが作成されると、プロキシは動的にフェールオーバー インターフェイスにバインドします。したがって、プロキシが何らかの理由でダウンすると、フェールオーバーがトリガーされます。

CARP には、ホスト用の 3 種類のステータスがあります。

- primary：各フェールオーバーグループのプライマリホストは 1 つだけです。
- backup
- init

CARP フェールオーバーグループ内のプライマリホストは、ローカルネットワークにアドバタイズメントを定期的に送信して、バックアップホストにまだ活動中であることを知らせます（このアドバタイズメント間隔は Web セキュリティアプライアンス で設定できます）。バックアップホストが（プロキシのダウン、Web セキュリティアプライアンス のダウンまたはネットワークからの切断が原因で）指定した期間中にプライマリからアドバタイズメントを受信しなかった場合は、フェールオーバーがトリガーされ、いずれかのバックアップがプライマリの役割を引き継ぎます。

プライマリ Web セキュリティアプライアンス からのアドバタイズメントは、次の条件を満たす場合、残りのバックアップホストに到達しません。

- ネットワークまたはインターフェイスが使用不可
- OS の正常性と可用性

（注） Web セキュリティアプライアンス の高可用性機能を使用するには、アプリケーションセントリックインフラストラクチャ（ACI）でデータプレーン IP ラーニングを無効にします。

（注） アプライアンス間のロードバランシング方式として高可用性を使用することはできません。デバイス間のトラフィックをロード バランシングするには、WCCP またはハードウェア ロード バランサを使用します。

次に、高可用性スイッチオーバーの原因となる設定を示します。

- 認証レルムの追加、削除、または更新
- ISE 設定の追加、削除、または更新
- HTTPS 証明書の追加または更新
- ログレベルの更新（プロキシログ）
- 透過的なリダイレクト設定の更新
- FTP プロキシの有効化、無効化、または更新
- SOCKS プロキシの有効化、無効化、または更新
- PAC ファイルの追加または変更
- アプライアンスからのインターフェイスの追加または削除
- フェールオーバーグループの追加または更新
- アップストリームプロキシの有効化または無効化
- WTT（Web トラフィックタップ）の有効化または無効化

フェールオーバー グループの追加

始める前に

- このフェールオーバー グループ専用に使用する仮想 IP アドレスを特定します。クライアントはこの IP アドレスを使用して、明示的な転送プロキシ モードでフェールオーバー グループに接続します。
- 以下のパラメータに対して、フェールオーバー グループ内のすべてのアプライアンスに同じ値を設定します。
  - フェールオーバー グループ ID（Failover Group ID）
  - ホストネーム

- 仮想 IP アドレス（Virtual IP Address）

- 仮想アプライアンスにこの機能を設定する場合は、各アプライアンス固有の仮想スイッチと仮想インターフェイスが無差別モードを使用するように設定されていることを確認します。詳細については、各自の仮想ハイパーバイザのマニュアルを参照してください。

ステップ 1 [ネットワーク（Network）] > [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 2 [フェールオーバーグループの追加（Add Failover Group）] をクリックします。

ステップ 3 [フェールオーバーグループ ID（Failover Group ID）] に 1 ～ 255 の値を入力します。

ステップ 4 （任意）[説明（Description）] に説明を入力します。

ステップ 5 [ホスト名（Hostname）] にホスト名を入力します（www.example.com など）。

ステップ 6 [仮想 IP アドレスとネットマスク（Virtual IP Address and Netmask）] に値を入力します。例：10.0.0.3/24（IPv4）または 2001:420:80:1::5/32（IPv6）。

ステップ 7 [インターフェイス（Interface）] メニューからオプションを選択します。[インターフェイスの自動選択（Select Interface Automatically）] オプションを選択すると、指定した IP アドレスに基づいてインターフェイスが選択されます。

（注） [インターフェイスの自動選択（Select Interface Automatically）] オプションを選択しない場合は、指定した仮想 IP アドレスと同じサブネット内のインターフェイスを選択する必要があります。

ステップ 8 優先順位を選択します。[プライマリ（Primary）] をクリックし、優先順位を 255 に設定します。または、[バックアップ（Backup）] を選択し、[優先順位（Priority）] フィールドに 1（最下位）～ 254 の優先順位を入力します。

ステップ 9 （任意）。サービスに対してセキュリティをイネーブルにするには、[サービスのセキュリティ有効化（Enable Security Service）] チェックボックスをオンにし、共有シークレットとして使用する文字列を [共有シークレット（Shared Secret）] と [共有シークレットの再入力（Retype Shared Secret）] フィールドに入力します。

（注） 共有シークレット、仮想 IP、フェールオーバー グループ ID は、フェールオーバー グループ内のすべてのアプライアンスで同一でなければなりません。

ステップ 10 [アドバタイズメントの間隔（Advertisement Interval）] フィールドに、アベイラビリティをアドバタイズするホスト間の遅延を秒単位（1 ～ 255）で入力します。

ステップ 11 変更を送信し、保存します。

次のタスク

関連項目

- フェールオーバーの問題

高可用性グローバル設定の編集

ステップ 1 [ネットワーク（Network）] > [ハイアベイラビリティ（High Availability）] を選択します。

ステップ 2 [高可用性グローバル設定（High Availability Global Settings）] 領域で、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [フェールオーバー処理（Failover Handling）] メニューからオプションを選択します。

- [プリエンプティブ（Preemptive）]：使用可能な場合、優先順位が最も高いホストが制御を担います。
- [プリエンプティブでない（Non-preemptive）]：より優先順が高いホストが使用可能になった場合でも、現在制御を担っているホストが制御を続行します。

ステップ 4 [送信（Submit）] をクリックします。または、[キャンセル（Cancel）] をクリックして変更を破棄します。

フェールオーバー グループのステータスの表示

[ネットワーク（Network）] > [ハイアベイラビリティ（High Availability）] を選択します。[フェールオーバーグループ（Failover Groups）] 領域に現在のフェールオーバー グループが表示されます。[ステータスの更新（Refresh Status）] をクリックすると、表示を更新できます。また、[ネットワーク（Network）]>[インターフェイス（Interfaces）] または [レポート（Report）] > [システム ステータス（System Status）] を選択すると、フェールオーバーの詳細を表示できます。

Web プロキシ データに対する P2 データ インターフェイスの使用

デフォルトでは、イネーブルになっている場合でも、Web プロキシは P2 で要求をリッスンしません。ただし、Web プロキシ データをリッスンするように P2 を設定できます。

（注） `advancedproxyconfig > miscellaneous` CLI コマンドを使用して、クライアント要求をリッスンするために P2 をイネーブルにする場合、発信トラフィックに P1 を使用するか、P2 を使用するかを選択できます。発信トラフィックに P1 を使用するには、データ トラフィックのデフォルト ルートを変更して、P1 インターフェイスが接続されている以下の IP アドレスを指定します。

始める前に

P2 をイネーブルにします（P1 がイネーブルになっていない場合は P1 もイネーブルにする必要があります）（ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）を参照）。

ステップ 1 CLI にアクセスします。

ステップ 2 `advancedproxyconfig > miscellaneous` コマンドを使用して、必要なエリアにアクセスします。

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

ステップ 3 []> **miscellaneous**

ステップ 4 下記の質問が表示されるまで、Enter キーを押して各質問をパスします。

```
Do you want proxy to listen on P2?
```

この質問に対して「**y**」を入力します。

ステップ 5 Enter キーを押して、残りの質問をパスします。

ステップ 6 変更を保存します。

次のタスク

関連項目

- アプライアンスの接続 （8 ページ）。
- TCP/IP トラフィック ルートの設定 （45 ページ）。
- トランスペアレント リダイレクションの設定 （48 ページ）

TCP/IP トラフィック ルートの設定

ルートは、ネットワーク トラフィックの送信先（ルーティング先）を指定するために使用されます。Web セキュリティアプライアンス は、以下の種類のトラフィックをルーティングします。

- **データ トラフィック。**Web を参照しているエンドユーザからの Web プロキシが処理するトラフィック。

- **管理トラフィック。**Webインターフェイスを介してアプライアンスを管理することによって作成されるトラフィック、およびアプライアンスが管理サービス（AsyncOSのアップグレード、コンポーネントのアップデート、DNS、認証など）用に作成するトラフィック。

デフォルトでは、どちらのトラフィックも、すべての設定済みネットワーク インターフェイス用に定義されたルートを使用します。ただし、管理トラフィックが管理ルーティング テーブルを使用し、データ トラフィックがデータ ルーティング テーブルを使用するように、ルーティングを分割することを選択できます。これらのトラフィックはそれぞれ以下のように分割されます。

管理トラフィック	データ トラフィック
• WebUI • SSH • SNMP • NTLM認証（ドメイン コントローラによる） • Syslogs • FTP プッシュ • DNS（設定可能） • アップデート/アップグレード/機能キー（設定可能）	• HTTP • HTTPS • FTP • WCCP ネゴシエーション • 外部 DLP サーバによる ICAP 要求 • DNS（設定可能） • アップデート/アップグレード/機能キー（設定可能） • LDAP/NTLM認証（ドメインコントローラにより設定可能）

[ネットワーク（Network）] > [ルート（Routes）] ページのセクションの数は、分割ルーティングがイネーブルかどうかに応じて決まります。

- **管理トラフィックとデータ トラフィック用の個別のルート設定セクション**（分割ルーティングがイネーブルの場合）。管理インターフェイスを管理トラフィック専用に使用する場合（[M1ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] がイネーブルの場合）、このページには、ルートを入力する 2 つのセクション（管理トラフィック用とデータ トラフィック用）が表示されます。
- **すべてのトラフィックに対して 1 つのルート設定セクション**（分割ルーティングがディセーブルの場合）。管理トラフィックとデータ トラフィックの両方に管理インターフェイスを使用する場合（[M1ポートをアプライアンス管理サービスのみに限定する（Restrict M1 port to appliance management services only）] がディセーブルの場合）、このページには、Webセキュリティアプライアンスから送信されるすべてのトラフィック（管理トラフィックとデータ トラフィックの両方）のルートを入力する 1 つのセクションが表示されます。

（注） ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。複数のポートがイネーブルになっている場合、Web プロキシは、データ トラフィック用に設定されているデフォルト ゲートウェイと同じネットワーク上のデータ インターフェイスでトランザクションを送信します。

発信サービス トラフィック

Web セキュリティアプライアンス は管理インターフェイスとデータ インターフェイスを使用して、サービス用の発信トラフィック（DNS、ソフトウェア アップグレード、NTP、traceroute データ トラフィックなど）もルーティングします。発信トラフィックに使用されるルートを選択することで、各サービスに対してこれを個々に設定できます。デフォルトでは、すべてのサービスに対して管理インターフェイスが使用されます。

関連項目

- 管理トラフィックとデータ トラフィックの分割ルーティングをイネーブルにするには、ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）を参照してください。

デフォルト ルートの変更

ステップ 1 [ネットワーク（Network）] > [ルート（Routes）] を選択します。

ステップ 2 必要に応じて、[管理（Management）] テーブルまたは [データ（Data）] テーブルの [デフォルト ルート（Default Route）] をクリックします（分割ルーティングがイネーブルになっていない場合は、統合された [管理/データ（Management/Data）] テーブル）。

ステップ 3 [ゲートウェイ（Gateway）] カラムで、編集するネットワーク インターフェイスに接続されているネットワークのネクスト ホップ上のコンピュータ システムの IP アドレスを入力します。

ステップ 4 変更を送信し、保存します。

ルートの追加

ステップ 1 [ネットワーク（Network）] > [ルート（Routes）] を選択します。

ステップ 2 ルートを作成するインターフェイスに対応する [ルートを追加（Add Route）] ボタンをクリックします。

ステップ 3 名前、宛先ネットワーク、およびゲートウェイを入力します。

ステップ 4 変更を送信し、保存します。

ルーティング テーブルの保存およびロード

[ネットワーク（Network）] > [ルート（Routes）] を選択します。

ルート テーブルを保存するには、[ルート テーブルを保存（Save Route Table）] をクリックし、ファイルの保存場所を指定します。

保存されているルート テーブルをロードするには、[ルート テーブルをロード（Load Route Table）] をクリックし、ファイルを探して開き、変更を送信して確定します。

（注） 宛先アドレスが物理ネットワーク インターフェイスの 1 つと同じサブネット上にある場合、AsyncOS は同じサブネット内のネットワーク インターフェイスを使用してデータを送信します。ルーティング テーブルは参照されません。

ルートの削除

ステップ 1 [ネットワーク（Network）] > [ルート（Routes）] を選択します。
ステップ 2 該当するルートの [削除（Delete）] 列のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックして確認します。
ステップ 4 変更を送信し、保存します。

次のタスク

関連項目

- ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）。

トランスペアレント リダイレクションの設定

- 透過リダイレクション デバイスの指定 （48 ページ）
- WCCP サービスの設定 （50 ページ）

透過リダイレクション デバイスの指定

始める前に

レイヤ 4 スイッチまたは WCCP v2 ルータにアプライアンスを接続します。

ステップ 1 [ネットワーク（Network）] > [トランスペアレント リダイレクション（Transparent Redirection）] を選択します。
ステップ 2 [デバイスの編集（Edit Device）] をクリックします。

ステップ 3 [タイプ（Type）] ドロップダウン リストから、アプライアンスに透過的にトラフィックをリダイレクトするデバイスのタイプとして [レイヤ 4 スイッチもしくはデバイスなし（Layer 4 Switch or No Device）] または [WCCP v2 ルータ（WCCP v2 Router）] を選択します。

ステップ 4 変更を送信し、保存します。

ステップ 5 WCCP v2 デバイスの場合は、以下の追加手順を実行します。

a) デバイスのマニュアルを参照して、WCCP デバイスを設定します。

b) Web セキュリティアプライアンス の [透過リダイレクション（Transparent Redirection）] ページで、[サービスの追加（Add Service）] をクリックし、WCCP サービスの追加と編集 （51 ページ）で説明している手順に従って WCCP サービスを追加します。

c) アプライアンスで IP スプーフィングがイネーブルになっている場合は、セカンド WCCP サービスを作成します。

次のタスク

関連項目

- アプライアンスの接続 （8 ページ）。
- WCCP サービスの設定 （50 ページ）。

L4 スイッチの使用

透過リダイレクションのためにレイヤ4スイッチを使用している場合、スイッチの設定によっては、Web セキュリティアプライアンス でいくつかの追加オプションを設定する必要があります。

- 通常は IP スプーフィングを有効にしないでください。アップストリーム IP アドレスのスプーフィングを行う場合は、非同期ルーティング ループを作成します。
- [Web プロキシ設定の編集（Edit Web Proxy Settings）] ページ（[セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）]）の[受信ヘッダーを使用する（Use Received Headers）] セクション（詳細設定）にある [X-Forwarded-For を使用したクライアント IP アドレスの識別を有効にする（Enable Identification of Client IP Addresses using X-Forwarded-For）] をオンにします。次に、1 つ以上の出力 IP アドレスを [信頼できるダウンストリーム プロキシまたはロード バランサ（Trusted Downstream Proxy or Load Balancer）] リストに追加します。
- 次に示すプロキシ関連パラメータを必要に応じて設定するには、CLI コマンド `advancedproxyconfig > miscellaneous` を使用できます。
  - `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)?` ：Web セキュリティアプライアンス がヘルスチェックに応答できるようにするには Y と入力します。
  - `Would you like proxy to perform dynamic adjustment of TCP receive window size?` ：ほとんどの場合はデフォルトの Y を使用します。Web セキュリティアプライアンス の別のプロキシ デバイス アップストリームがある場合は N と入力します。

- `Do you want to pass HTTP X-Forwarded-For headers?` ：X-Forwarded-For（XFF）ヘッダーの要件アップストリームがない場合は不要です。
- `Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?` ：トラブルシューティングを支援するには Y と入力できます。クライアント IP アドレスがアクセス ログに表示されます。
- `Would you like the proxy to use client IP addresses from X-Forwarded-For headers?` ポリシー設定とレポートを支援するには Y と入力できます。

- X-Forwarded-For（XFF）ヘッダーを使用する場合は、XFF ヘッダーをログに記録するため、アクセス ログ サブスクリプションに `%f` を追加します。W3C ログ形式の場合は `cs(X-Forwarded-For)` を追加します。

WCCP サービスの設定

WCCP サービスは、WCCP v2 ルータにサービス グループを定義するアプライアンスの設定です。使用するサービス ID やポートなどの情報が含まれます。サービス グループを使用して、Web プロキシは WCCP ルータとの接続を確立し、ルータからリダイレクトされたトラフィックを処理することができます。

WCCP プロキシのヘルスチェックがイネーブルの場合、Web セキュリティアプライアンス の WCCP デーモンは Web プロキシサーバーで実行されている xmlrpc サーバーに 10 秒おきにヘルスチェックメッセージ（xmlrpc クライアント要求）を送信します。プロキシが稼働している場合、WCCP サービスはプロキシから応答を受信し、Web セキュリティアプライアンス は指定された WCCP 対応ルータに WCCP「here I am」（HIA）メッセージを 10 秒おきに送信します。WCCP サービスがプロキシから応答を受信しない場合、HIA メッセージは WCCP ルータに送信されません。

WCCP ルータが HIA メッセージを 3 回連続して受信しなかった場合、ルータはサービスグループから Web セキュリティアプライアンス を削除し、Web セキュリティアプライアンス にトラフィックが転送されないようになります。

CLI コマンド `advancedproxyconfig > miscellaneous > Do you want to enable WCCP proxy health check?` を使用して、プロキシ ヘルス チェック メッセージをイネーブルまたはディセーブルすることができます。ヘルス チェックはデフォルトでディセーブルです。

（注） WCCPv2 サービスは、IPv4 ネットワークおよび IPv6 ネットワークで動作します。1 つのアプライアンスに最大 15 個のサービス グループを設定できます。WCCP ルータの各サービスグループには、最大 32 のアプライアンスを含めることができます。WCCPv2 サービスは、ロード バランシング メカニズムにも使用され、コンテンツエンジンの過負荷とデータブロッキングを軽減します。

（注） 同じアプライアンスで WCCP とハイアベイラビリティを設定することはサポートされていません。設定されている場合、Web セキュリティアプライアンス は期待どおりに機能しません。

- WCCP ロード バランシングについて （51 ページ）
- WCCP サービスの追加と編集 （51 ページ）
- IP スプーフィングの WCCP サービスの作成 （56 ページ）

WCCP ロード バランシングについて

WCCP サービス定義の [割り当ての重み付け（Assignment Weight）] パラメータは、この Web セキュリティアプライアンス が WCCP プールのメンバーまたはサービスグループとして動作している場合に、WSA の負荷を調整するために使用されます。この重み付けは、処理するためにこの Web セキュリティアプライアンス に送信できる WCCP の合計トラフィックに対する比率を表します。

割り当ての重み付けを調整する必要があるのは、さまざまなタイプのゲートウェイアプライアンスが同じ WCCP プールのメンバーになっていて、強力なアプライアンスに振り分けるトラフィックの量を増やす必要がある場合のみです。

（注） WCCP プールのメンバーになっているすべての Web セキュリティアプライアンス で、WCCP ロードバランシングを利用するには、割り当ての重み付けをサポートする AsyncOS のバージョンが実行されている必要があります。

（注） WCCP は、最大 32 のアプライアンスの透過的なトラフィックを負荷分散します。ハッシュまたはマスクに基づいてトラフィックフローのバランスをとり、ネットワークに複数のアプライアンスモデルが存在する場合はトラフィックが重み付けされます。ダウンタイムなしでサービスプールにデバイスを追加したり、サービスプールからデバイスを削除したりできます。ただし、8 つ以上のアプライアンスを使用している、または使用する予定の場合は、専用のロードバランサを用意することをお勧めします。

[割り当ての重み付け（Assignment Weight）] パラメータの詳細については、WCCP サービスの追加と編集 （51 ページ）を参照してください。

WCCP サービスの追加と編集

始める前に

WCCP v2 ルータを使用するようにアプライアンスを設定します（透過リダイレクション デバイスの指定 （48 ページ）を参照）。

ステップ 1 [ネットワーク（Network）] > [透過リダイレクション（Transparent Redirection）] を選択します。

ステップ 2 [サービスの追加（Add Service）] をクリックします。または、WCCP サービスを編集するには、[サービスプロファイル名（Service Profile Name）] 列にある WCCP サービスの名前をクリックします。

ステップ 3 以下の手順に従って、WCCP のオプションを設定します。

WCCP サービス オプション	説明
サービス プロファイル名（Service Profile Name）	WCCP サービスの名前。 （注） このオプションを空のままにして、標準サービス（下記を参照）を選択すると、「web_cache」という名前が自動的に割り当てられます。

WCCP サービス オプション	説明
サービス	ルータのサービス グループのタイプ。次から選択します。 **[標準サービス（Standard service）]。**このサービス タイプには、固定 ID「ゼロ」、固定リダイレクト方式「宛先ポート別」、固定宛先ポート「80」が割り当てられます。1 つの標準サービスのみ作成できます。アプライアンスに標準サービスがすでに存在している場合、このオプションはグレー表示されます。 **[ダイナミックサービス（Dynamic service）]。**このサービス タイプでは、カスタム ID、ポート番号、およびリダイレクト オプションとロード バランシング オプションを定義できます。WCCP ルータでサービスを作成するときは、ダイナミック サービスで指定したパラメータと同じパラメータを入力します。 ダイナミック サービスを作成する場合は、以下の情報を入力します。 • **[サービス ID（Service ID）]。**[ダイナミックサービス ID（Dynamic Service ID）] フィールドに 0 ～ 255 の任意の数字を入力できます。ただし、このアプライアンスには 15 個以上のサービス グループを設定することはできません。 • **[ポート番号（Port number(s)）]。**[ポート番号（Port Numbers）] フィールドにリダイレクトするトラフィックに最大 8 つのポート番号を入力します。 • **[リダイレクションの基礎（Redirection basis）]。**送信元ポートまたは宛先ポートに基づいてトラフィックをリダイレクトするように選択します。デフォルトは宛先ポートです。 （注） 透過リダイレクションと IP スプーフィングを使用してネイティブ FTP を設定するには、[ソースポート（リターンパス）に基づいてリダイレクト（Redirect based on source port (return path)）] を選択し、送信元ポートを 13007 に設定します。 • **[ロード バランシングの基礎（Load balancing basis）]。**ネットワークが複数の Web セキュリティアプライアンス を使用している場合、アプライアンス間でパケットを配布する方法を選択できます。サーバまたはクライアントアドレスに基づいてパケットを配布できます。クライアントアドレスを選択した場合、クライアントからのパケットは常に同じアプライアンスに配布されます。デフォルトはサーバアドレスです。
ルータ IP アドレス	1 つまたは複数の WCCP 対応ルータの IPv4 または IPv6 アドレスを入力します。各ルータ固有の IPを使用します。マルチキャストアドレスは入力できません。1 つのサービス グループ内に IPv4 と IPv6アドレスを混在させることはできません。

WCCP サービス オプション	説明
ルータ セキュリティ	このサービス グループに対してパスフレーズを要求する場合は、[サービスのセキュリティ有効化（Enable Security for Service）] をオンにします。イネーブルにした場合、そのサービス グループを使用するアプライアンスと WCCP ルータは同じパスフレーズを使用する必要があります。 使用するパスフレーズと確認パスフレーズを入力します。

WCCP サービス オプション	説明
詳細設定（Advanced）	**ロード バランシング方式。**複数の Web セキュリティアプライアンス 間においてルータがパケットのロードバランシングを実行する方法を決定します。次から選択します。 • **[マスクのみ許可（Allow Mask Only）]。**WCCP ルータは、ルータのハードウェアを使用して決定を行います。この方式は、ハッシュ方式よりもルータのパフォーマンスを向上させます。ただし、すべての WCCP ルータがマスク割り当てをサポートしているわけではありません。（IPv4 のみ） • **[ハッシュのみ許可（Allow Hash Only）]。**この方式は、ハッシュ関数に依存して、リダイレクションに関する決定を下します。この方式はマスク方式ほど効率的ではありませんが、ルータがこのオプションしかサポートしていない場合もあります。（IPv4 および IPv6） • **[ハッシュもしくはマスクを許可（Allow Hash or Mask）]。**AsyncOS がルータと方式をネゴシエートできるようになります。ルータがマスクをサポートしている場合、AsyncOS はマスクを使用します。サポートしていない場合は、ハッシュが使用されます。 **[マスクのカスタマイズ（Mask Customization）]。**[マスクのみ許可（Allow Mask Only）] または [ハッシュのみ許可（Allow Hash Only）] を選択する場合、マスクをカスタマイズしたり、ビット数を指定したりできます。 • **[カスタム マスク（最大 6 ビット）]。**マスクを指定できます。Web インターフェイスは、提供するマスクに関連付けられたビット数を表示します。IPv4 ルータの場合は最大 5 ビット、IPv6 ルータの場合は最大 6 ビットを使用できます。 • **[システム生成マスク（System generated mask）]。**システムがマスクを生成するように設定できます。任意で、システムにより生成されたマスクにビット数（1 ～ 5）を指定できます。 **[重みの割り当て（Assignment Weight）]**：この Web セキュリティアプライアンス の WCCP 重み付け。有効な値は 0 ～ 255 です。この重み付けは、WCCP サービスグループのメンバーとしてのこの Web セキュリティアプライアンス に送信して処理できる合計トラフィックに対する比率を表します。ゼロの値は、この Web セキュリティアプライアンス はサービスグループのメンバーであっても、ルータからリダイレクトされるトラフィックを受信しないことを意味します。詳細については、WCCP ロードバランシングについて （51 ページ）を参照してください。 **[転送方式（Forwarding method）]。**この方式では、リダイレクトされたパケットがルータから Web プロキシに転送されます。 **[リターン方式（Return Method）]。**この方式では、リダイレクトされたパケットが Web プロキシからルータに転送されます。

WCCP サービス オプション	説明
	転送方式およびリターン方式では、以下のいずれかのメソッドタイプが使用されます。 • **[レイヤ 2（L2）（Layer 2 (L2)）]**。パケットの宛先 MAC アドレスをターゲット Web プロキシの MAC アドレスに置き換えることで、レイヤ2のトラフィックをリダイレクトします。L2メソッドはハードウェア レベルで動作し、通常、最高のパフォーマンスを実現します。ただし、すべての WCCP ルータが L2 転送をサポートしているわけではありません。また、WCCPルータは、（物理的に）直接接続されている Web セキュリティアプライアンス との L2 ネゴシエーションのみを許可します。 • [総称ルーティングカプセル化（GRE）（Generic Routing Encapsulation (GRE)）]。この方式は、GRE ヘッダーとリダイレクト ヘッダーを含むIPパケットをカプセル化することで、レイヤ3でトラフィックをリダイレクトします。GRE はソフトウェア レベルで動作し、パフォーマンスに影響する可能性があります。 • **[L2 またはGRE（L2 or GRE）]**。このオプションを指定すると、アプライアンスはルータがサポートしている方式を使用します。ルータとアプライアンスの両方が L2 と GRE をサポートする場合、アプライアンスは L2 を使用します。 ルータが直接アプライアンスに接続されていない場合、GRE を選択する必要があります。

ステップ 4 変更を送信し、保存します。

IP スプーフィングの WCCP サービスの作成

ステップ 1 Web プロキシで IP スプーフィングがイネーブルになっている場合は、2 つの WCCP サービスを作成します。標準の WCCP サービスを作成するか、宛先ポートに基づいてトラフィックをリダイレクトするダイナミック WCCP サービスを作成します。

ステップ 2 宛先ポートに基づいてトラフィックをリダイレクトするダイナミック WCCP サービスを作成します。

ステップ 1 で作成したサービスで使用されるポート番号、ルータ IP アドレス、ルータ セキュリティの設定と同じ設定を使用します。

（注）
- シスコでは、リターン パスに使用する（送信元ポートに基づく）WCCP サービスには 90 ～ 97 のサービス ID 番号を使用することを推奨します。
- WCCP ロードバランシング方式を [マスクのみ許可（Allow Mask Only）]または [ハッシュもしくはマスクを許可（Allow Hash or Mask）] に設定して、複数のアプライアンスにトラフィックを分散する場合は、なりすましの IP アドレスを適切に設定します。なりすましの IP アドレスの設定では、WCCP ルータと Web セキュリティアプライアンス 間のトラフィックを適切にルーティングする必要があります。

次のタスク

関連項目

- Web プロキシ キャッシュ。

VLAN の使用によるインターフェイス能力の向上

1 つまたは複数の VLAN を設定することで、組み込まれている物理インターフェイスの数を超えて、Web セキュリティアプライアンス が接続可能なネットワークの数を増加できます。

VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データ ポート」として表示されます。「DDDD」は最大 4 桁の ID です（VLAN 2、VLAN 4094 など）。AsyncOS は、最大 30 の VLAN をサポートします。

物理ポートは、VLAN に配置するために IP アドレスを設定する必要がありません。VLAN を作成した物理ポートに VLAN 以外のトラフィックを受信する IP アドレスを設定できるため、VLAN のトラフィックと VLAN 以外のトラフィックの両方を同じインターフェイスで受信できます。

VSAN の設定と管理

VLAN の作成、編集、および削除を行うには、`etherconfig` コマンドを使用します。作成した VLAN は、CLI の `interfaceconfig` コマンドを使用して設定できます。

（注） VLAN 設定を変更する場合は、必ずアプライアンスをリブートしてください。

例 1：**新しい VLAN の作成**

この例では、P1 1 ポート上に 2 つの VLAN（VLAN 31 と VLAN 34）を作成します。

（注） T1 または T2 インターフェイス上で VLAN を作成しないでください。

ステップ 1 CLI にアクセスします。

ステップ 2 以下の手順を実行します。

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN   31 (P1)
2. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
```

ステップ 3 変更を保存します。

例 2 : VLAN 上の IP インターフェイスの作成

この例では、VLAN 34 イーサネット インターフェイス上に新しい IP インターフェイスを作成します。

（注） インターフェイスに変更を加えると、アプライアンスとの接続が閉じることがあります。

ステップ 1 CLI にアクセスします。

ステップ 2 以下の手順を実行します。

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new
IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10
Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN   34
[1]> 4
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>
Hostname:
[]> v.example.com
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN   34 (10.10.31.10 on VLAN  34: v.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
example.com> commit
```

ステップ 3 変更を保存します。

次のタスク

関連項目

- ネットワーク インターフェイスのイネーブル化または変更 （26 ページ）。
- TCP/IP トラフィック ルートの設定 （45 ページ）。

リダイレクト ホスト名とシステム ホスト名

システム セットアップ ウィザードを実行すると、システム ホスト名とリダイレクト ホスト名が同一になります。ただし、`sethostname` コマンドを使用してシステムのホスト名を変更しても、リダイレクト ホスト名は変更されません。そのため、複数の設定に異なる値が含まれることになります。

AsyncOS は、エンドユーザー通知と応答確認にリダイレクト ホスト名を使用します。

システム ホスト名は、次のエリアでアプライアンスの識別に使用される完全修飾ホスト名です。

- コマンドライン インターフェイス（CLI）
- システム アラート
- Web セキュリティアプライアンス が Active Directory ドメインに参加するときに、マシンの NetBIOS 名を作成する場合

システムホスト名はインターフェイスのホスト名と直接対応しておらず、クライアントがアプライアンスに接続するために使用されません。

リダイレクト ホスト名の変更

ステップ 1 Web ユーザー インターフェイスで、[ネットワーク（Network）] > [認証（Authentication）] に移動します。
ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。
ステップ 3 [リダイレクトホスト名（Redirect Hostname）] に新しい値を入力します。

システム ホスト名の変更

ステップ 1 CLI にアクセスします。
ステップ 2 Web セキュリティアプライアンス の名前を変更するには、`sethostname` コマンドを使用します。

```
example.com> sethostname

example.com> hostname.com

example.com> commit
...
hostname.com>
```

ステップ 3 変更を保存します。

SMTP リレー ホストの設定

AsyncOS は、通知、アラート、Cisco IronPort カスタマー サポート要求など、システムにより生成された電子メール メッセージを定期的に送信します。デフォルトでは、AsyncOS はドメインの MX レコードにリストされている情報を使用して電子メールを送信します。ただし、アプライアンスが MX レコードにリストされているメール サーバーに直接到達できない場合、アプライアンス上に少なくとも 1 つの SMTP リレー ホストを設定します。

（注） Web セキュリティアプライアンス が MX レコードまたは設定済み SMTP リレー ホストにリストされているメール サーバと通信できない場合、電子メール メッセージを送信できず、ログ ファイルにメッセージを書き込みます。

1 つまたは複数の SMTP リレー ホストを設定できます。複数の SMTP リレー ホストを設定する場合、AsyncOS は、使用可能な最上位の SMTP リレー ホストを使用します。SMTP リレー ホストが使用できない場合、AsyncOS は、そのリスト 1 つ下のリレー ホストの使用を試みます。

SMTP リレー ホストの設定

ステップ 1 [ネットワーク（Network）] > [内部SMTPリレー（Internal SMTP Relay）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [内部SMTPリレー（Internal SMTP Relay）] の設定を完成させます。

プロパティ	説明
リレーホスト名または IP アドレス（Relay Hostname or IP Address）	SMTP リレーに使用するホスト名または IP アドレス。
ポート（Port）	SMTP リレーに接続するためのポート。このプロパティを空欄にした場合、アプライアンスはポート 25 を使用します。
SMTP への接続に使用するルーティング テーブル（Routing Table to Use for SMTP）	SMTP リレーへの接続に使用するアプライアンスのネットワーク インターフェイス（管理またはデータのいずれか）に関連付けられているルーティング テーブル。リレー システムと同じネットワークにあるインターフェイスを選択します。

ステップ 4 （任意）[行を追加（Add Row）] をクリックして別の SMTP リレー ホストを追加します。

ステップ 5 変更を送信し、保存します。

DNS の設定

AsyncOS for Web は、インターネット ルート DNS サーバまたはユーザ独自の DNS サーバを使用できます。インターネット ルート サーバを使用する場合、特定のドメインに使用する代替サーバを指定できます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

セカンダリ DNS ネーム サーバを指定して、プライマリ ネーム サーバで解決されないクエリを解決することもできます。セカンダリ DNS サーバはフェールオーバー DNS サーバとして使用

されません。プライマリ DNS サーバからDNS 設定の編集 （62 ページ）で指定されたエラーが返された場合は、優先順位に従ってセカンダリ DNS サーバがクエリされます。

認証の失敗を防ぐには、Web セキュリティアプライアンス 認証リダイレクト名が一意であることを確認してください。

- スプリット DNS （62 ページ）
- DNS キャッシュのクリア （62 ページ）
- DNS 設定の編集 （62 ページ）

スプリット DNS

AsyncOS は、内部サーバが特定のドメインに設定され、外部またはルート DNS サーバが他のドメインに設定されたスプリット DNS をサポートします。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

DNS キャッシュのクリア

始める前に

このコマンドを使用すると、キャッシュの再投入中に一時的にパフォーマンスが低下することがあるので注意してください。

ステップ 1 [ネットワーク（Network）] > [DNS] を選択します。

ステップ 2 [DNSキャッシュを消去（Clear DNS Cache）] をクリックします。

DNS 設定の編集

ステップ 1 **[ネットワーク（Network）] > [DNS]** を選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 必要に応じて、DNS 設定値を設定します。

プロパティ	説明
プライマリ DNS サーバ（Primary DNS Servers）	**[これらのDNSサーバを使用（Use these DNS Servers）]**。アプライアンスがホスト名の解決に使用できるローカル DNS サーバ。 [優先代替DNSサーバ（オプション）（Alternate DNS servers Overrides (Optional)）]。特定のドメイン用の権威 DNS サーバ **[インターネットのルートDNSサーバを使用（Use the Internet's Root DNS Servers）]**。アプライアンスがネットワーク上のDNSサーバにアクセスできない場合に、ドメイン名サービス ルックアップにインターネットのルート DNS サーバを使用することを選択できます。 （注） インターネット ルート DNS サーバは、ローカル ホスト名を解決しません。アプライアンスでローカル ホスト名を解決する必要がある場合は、ローカル DNS サーバを使用して解決するか、コマンドライン インターフェイスからローカル DNS に適切なスタティック エントリを追加する必要があります。これは、新しい Web インターフェイスにアクセスするためにも必要です。
セカンダリ DNS サーバ（Secondary DNS Servers）	プライマリ ネーム サーバで解決されなかったホスト名を解決するためにアプライアンスが使用できるセカンダリ DNS サーバ。 （注） プライマリ DNS サーバから次のエラーが返されると、セカンダリ DNS サーバがホスト名クエリを受信します。 • エラーなし、応答セクションを受信しませんでした。（No Error, no answer section received.） • サーバが要求を完了できませんでした。応答セクションがありません。（Server failed to complete request, no answer section.） • 名前エラー、応答セクションを受信しませんでした。（Name Error, no answer section received.） • 実装されていない機能です。（Function not implemented.） • サーバがクエリへの応答を拒否しました。（Server Refused to Answer Query.）
DNS トラフィック用ルーティングテーブル（Routing Table for DNS Traffic）	DNS サービスがルート トラフィックをルーティングする際に経由するインターフェイスを指定します。
IP アドレス バージョン設定（IP Address Version Preference）	DNS サーバが IPv4 と IPv6 の両方のアドレスを提供する場合、AsyncOS はこの設定を使用して IP アドレスのバージョンを選択します。 （注） AsyncOS は、透過的 FTP 要求のバージョン設定に従いません。

プロパティ	説明
DNS 逆引きタイムアウト（Wait Before Timing out Reverse DNS Lookups）	無応答逆引き DNS ルックアップがタイムアウトするまでの待機時間（秒単位）。
ドメイン検索リスト（Domain Search List）	簡易ホスト名（「.」記号がないホスト名）宛てに要求を送信する際に使用される DNS ドメイン検索リスト。ドメイン名を加えたホスト名に一致する DNS が存在するどうかを調べるために、指定されたドメインが入力順に照合されます。

ステップ 4 変更を送信し、保存します。

次のタスク

関連項目

- TCP/IP トラフィック ルートの設定 （45 ページ）
- IP アドレスのバージョン （25 ページ）

接続、インストール、設定に関するトラブルシューティング

- フェールオーバーの問題
- アップストリーム プロキシが基本クレデンシャルを受け取らない
- クライアント要求がアップストリーム プロキシで失敗する
- 最大ポート エントリ数

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