CHAPTER 2

インストールの計画

この章では、Cisco ACE XML ゲートウェイ および Manager アプライアンスのインストールを計画する際の考慮事項について説明します。内容は次のとおりです。

ターゲット ネットワークのインストールに関する考慮事項

ACE XML Gateway の日常的な運用には、さまざまなアグリーメント、プロトコル、および物理接続が必要となります。ACE XML Gateway の導入には、アプライアンスそのものの設定だけでなく、アプライアンスをターゲット ネットワークに組み入れるための設定が必要です（たとえば、隣接するファイアウォールまたはリモートのネットワーク管理デバイスを設定します）。

アプライアンスをインストールする環境としては、次のようないくつかのタイプがあります。

- 稼動環境では、1 つ以上の ACE XML Gateway をネットワーク DMZ（通常はロード バランサの後ろ側）に配置するのが一般的です。この設定では、Gateway はネットワーク外部からのクライアント要求を受信し、これらの要求をロード バランサを経由して組織内の宛先サーバに返します。
- ポリシーの作成またはテストの間は、通常では ACE XML Gateway は保護されたネットワーク内に存在します。
- ACE XML Manager は通常、内部の保護されたネットワーク内に存在し、外部トラフィックとは接触しません。ただし、各 ACE XML Gateway に接続できるようにする必要があり、またポリシー作成者が使用できるようにする必要もあります。

稼動環境では、ACE XML Gateway および Manager は、通常では外部ネットワークへのアクセスを必要とします。ネットワーク トポロジによっては、アプライアンスの発信 HTTP プロキシの設定が必要になる場合があります。ACE XML Gateway および Manager はすべてのアウトバウンドの HTTP 接続にプロキシを使用します。Gateway および Manager アプライアンスの HTTP プロキシの設定は、Web コンソールの [System Management] ページで個別に実行できます。詳細については、Web コンソールから使用できる Manager オンライン ヘルプを参照してください。

ACE XML Gateway および Manager が使用するポート

ネットワークでアプライアンスが正常に機能するには、既存のネットワーク デバイス（内部ファイアウォールなど）で、このアプライアンスが使用するトラフィック タイプを許可されている必要があります。

ACE XML Gateway および Manager のインストールによって影響されるファイアウォールは、具体的には次のとおりです。

- 各 ACE XML Gateway と、これを制御する Manager の間にあるファイアウォール。
- Manager と、Web コンソールへのアクセスに使用するコンピュータの中間にあるファイアウォール。
- Gateway と外部ネットワークの中間にあるファイアウォール。

次の各項で、開放する必要があると考えられるポートを示します。

システム トラフィック用のポート

次のポートは、システムの動作（つまり、サービス トラフィック以外のトラフィック）に使用されます。ここで示す情報は、内部ファイアウォールの設定に使用します。ポートの使用法は、実装ごとに異なります。たとえば、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用しない場合には、ポート 123 で TCP/UDP トラフィックを許可するようにファイアウォールを設定する必要はありません。

ACE XML Manager は、次のポートおよびプロトコルを使用します。

- ICMP（任意のデバイスから）
- ポート 22、TCP（任意のデバイスから）。このポートは、Manager で端末セッションを起動する管理者向けに SSH 接続を提供します。
- ポート 8243、TCP（任意のデバイスから）。このポートは、ブラウザ アクセス用に Manager の Web コンソール接続を提供します。

  上記以外のポートで Web コンソールを提供するように Manager を設定することも可能です。
- ポート 53、UDP（任意のデバイスから）。Manager は、このポートを使用して DNS ルックアップを実行します。
- ポート 161、UDP（任意のデバイスから）。Manager はこのポートによって SNMP クエリーを受信できます。
- ポート 514、UDP（ACE XML Gateway から）。Manager は、このポートをリッスンして Gateway から Syslog 情報を受信します。この情報を集約してイベント ログが作成されます。

Gateway では、次のポートおよびプロトコルを使用してトラフィックの送受信を行います。

- ICMP（任意のデバイスから）
- ポート 22、TCP（任意のデバイスから）。このポートは、Gateway で端末セッションを起動する管理者向けに SSH 接続を提供します。
- ポート 8200、TCP（Manager 以外からは不可）。Gateway が対応する Mananger から制御メッセージを受信できるよう、このポートを開放する必要があります。
- ポート 53、UDP（任意のデバイスから）。Gateway はこのポートによって DNS ルックアップを実行できます。
- ポート 161、UDP（任意のデバイスから）。Gateway はこのポートによって SNMP クエリーを受信できます。

各 Gateway が Manager に送信するトラフィックは、その目的のために Manager 上で開放されているポートに送信されます。これに加え、Manager と Gateway アプライアンスは、次のポートでネットワーク トラフィックを生成する場合があります。

- ポート 123、TCP/UDP（NTP 用）。
- ポート 25、TCP（SMTP 経由での電子メール アラートの送信用）。
- ポート 162、UDP（SNMP トラップ用）。

サービス トラフィック用のポート

「システム トラフィック用のポート」（P.2-2）で説明されているシステム トラフィックに必要なポートでトラフィックを許可することに加えて、ファイアウォールは ACE XML Gateway ポリシーで設定されているサービス ポートでのトラフィックを許可する必要があります。

サービス トラフィックに使用するポートはポリシーによって異なりますが、一般にポート 80 および 443（それぞれ標準の HTTP および HTTPS トラフィックに対応）を含めます。

ロード バランサに関する考慮事項

通常、1 つまたは複数のロード バランサ デバイスの後ろ側に複数の ACE XML Gateway を配置すると、最良のパフォーマンスが得られます。専用 Manager は大量のトラフィックを処理することが少ないため、通常ではこの前にロード バランサを配置する必要はありません。

ロード バランサは Gateway の可用性を高める場合、または作業負荷を分散させる場合に使用します。使用するロード バランサの数は、各 Gateway が処理すると見込まれるトラフィック量のほか、ロード バランサの仕様によって左右されます。必要なロード バランサ数を決定する際に支援が必要であれば、ロード バランサの製造元に問い合わせてください。

一般には、ACE XML Gateway にロード バランサを設定する手順は、Web サーバにロード バランシングを設定する場合と同様です。クラスタ内の各 Gateway にメッセージをルーティングするための、任意のメッセージ アロケーション方式を使用して、ロード バランサで Gateway クラスタに Virtual IP（VIP; 仮想 IP）を設定します。

ロード バランサが Gateway の状態を監視できるようにする必要があります。ACE XML Gateway はアプリケーションレベルの監視をサポートしています。ロード バランサは Gateway に HTTP 要求（HEAD または GET）を送信し、アプライアンスの状態を示す HTML ページまたはその他のタイプの応答を受信できます。HEAD メソッド要求は最小の帯域幅を使用してシステム ヘルスをチェックできるため、多くの場合では HEAD メソッド要求の使用が適しています。

（注） ロード バランサもまた *ping* メッセージを使用して ACE XML Gateway の応答性をチェックできます。ただし、HTTP 要求の使用により Gateway での高度なプロセスがアクティブになります。

Gateway ポリシーで、ポート オブジェクトに [HTTP health check] ページ（固定応答メッセージ）を設定します。ポリシーでポート オブジェクトにヘルス チェック応答を設定する詳細については、『*Cisco ACE XML Gateway User Guide*』の「Working with Ports and Hostnames」の章を参照してください。

ポリシーのポート オブジェクトは、通常では 1 つのポート番号をリッスンし、また 1 つ以上の VIP アドレスまたはホスト名に対して設定されています。ポート設定のホスト名は、クライアントまたは上流のロード バランサが Gateway へのサービス トラフィックを処理する際に使用します。各 Gateway の物理インターフェイスを特定の IP アドレスに対して設定する必要もあります。

ポート オブジェクトにはアプリケーションの要求をリッスンする複数の IP アドレスを設定できますが、Gateway は物理インターフェイスが設定されていないポート オブジェクトの IP アドレスを無視します。次の設定例では、Gateway で指定されたポート番号で複数のアプリケーションが使用可能な場合に、このようなポート オブジェクトの IP アドレスを使用して要求を明確にする方法を説明しています。

ここでは、3 つの Web アプリケーションをデフォルトの HTTPS ポートである 443 で使用可能にする必要がある 2 つの Gateway のクラスタについて考えます。指定された仮想ホスト名に関連付けられている証明書（および鍵）を SSL ハンドシェイク時に選択する必要があるため（クライアントの Host ヘッダーが出現する前）、要求のターゲットとなるアプリケーションを IP アドレスを使用して明確にする必要があります。この例を導入するために、各 Gateway の物理インターフェイスに 3 つの IP アドレス（各アプリケーションに 1 つずつ）を指定できます。たとえば、Gateway A には 10.0.2.5–7 を、また Gateway B には 10.0.3.5–7 を指定できます。Web サイト https://example.com を Gateway A では 10.0.2.5 に、または Gateway B では 10.0.3.5 に設定できます。このため、Web サイト https://example.com に使用する HTTP ポートは、10.0.2.5 および 10.0.3.5 を要求をリッスンする IP アドレスとして指定する必要があります（他の 2 つのアプリケーションに使用するポートは、各 Gateway で他の 2 つのアドレスをリッスンします）。

プロキシ サーバ経由での Web コンソール アクセスの有効化

システムの主要開発環境は、ポリシーを作成するためのブラウザベースのインターフェイスである、Manager の Web コンソールです。組織のポリシー作成者は、自身の作業環境から Web コンソールにアクセスできる必要があります。転送プロキシ サーバがクライアントの Web アクセスに使用されている場合には、設定を変更してプロキシ サーバを受け入れる必要がある場合があります。

デフォルトでは、Manager の Web コンソールはポート 8243（ポート 443 は Web サービス トラフィックが使用できるように空けておきます）で動作します。インストール後、ポリシー作成者が、8243 へのアクセスを許可しないプロキシ サーバを使用するように設定されたブラウザで Manager に接続しようとすると、「permission denied」エラーが発生します。

プロキシ サーバをポート 8243 で Manager アプライアンスにアクセスできるように設定することで、この問題を修正できます。また、Web コンソールを 8243 以外のポートで使用できるように Manager を設定することも可能です。これ以外の方法としては、Web コンソールにアクセスする必要があるブラウザを、Web コンソール接続時にプロキシ サーバを迂回するように設定する方法があります。

アプライアンスのネットワーク インターフェイスに関する考慮事項

Cisco ACE XML ゲートウェイ アプライアンスは、ネットワーク通信にイーサネットを使用します。イーサネット以外のネットワーク（トークン リング、PS/2 ネットワークなど）はサポートしていません。最高のギガビット イーサネット パフォーマンスを達成するには、ネットワークを構成するケーブルの規格が CAT 5e 以上であることが必要です。このアプライアンスでは、標準の RJ-45 イーサネット コネクタを使用できます。

この 1U のプラットフォームには、サービス トラフィックを受信できる 4 つのネットワーク インターフェイスが装備されています（追加の RJ-45 インターフェイスは、Integrated Lights-Out（iLO）モジュールの接続専用です）。これらのインターフェイスは、全二重モードの 10BASE-T、100BASE-T、またはギガビット イーサネット速度で動作するように設定できます。

この設定を自動的にネゴシエートするようにインターフェイスを設定できますが、自動ネゴシエートを回避し、各インターフェイスが固有の速度で動作するように設定すれば、最良のパフォーマンスが得られます。このように推奨する理由は、帯域幅の設定を自動ネゴシエートするために費やされる時間に

よって、少量とはいえパフォーマンス オーバーヘッドが生じるからです。ネットワーク条件の変化によって、帯域幅の設定についての不要な再ネゴシエーションが行われる可能性があり、これもパフォーマンス低下につながります。帯域幅の自動ネゴシエートを使用すると、他のネットワーク デバイス（ファイアウォール、ルータなど）に問題が発生した場合に、パフォーマンスの低下が伝播する可能性があります。1 台のルータが故障すると、理論上、そのルータと連携し自動ネゴシエートを実行しているすべての ACE XML Gateway で全トラフィックにボトルネックが発生し、故障したルータと無関係なゾーンでも速度が低下する可能性があります。

自動ネゴシエートを使用すると、パフォーマンス問題の原因を特定するのが困難になる場合が多くなりますが、プリセットの帯域幅設定を使用すると、動作不良のルータ、ファイアウォール、または ACE XML Gateway を迅速に特定しやすくなります。

IP アドレス要件

モデルに応じて、アプライアンス シャーシには最大 5 つのイーサネット ポートがあります。iLO ポートは管理目的だけに使用し、サービス トラフィックには使用しません。

通常、ACE XML Gateway のトラフィック処理には、1 つのインターフェイスと IP アドレスを使用するだけで十分です。場合によっては、管理者が Gateway 宛てのサービス トラフィックを Manager トラフィックから分離し、2 つの異なるイーサネット ポートに振り分けることもできます。ただし、これはセキュリティの強化を目的とするオプションの設定です。

もう 1 つの設定オプションとして、1 つの特定の Gateway インターフェイスに対応付けられた複数の IP アドレスを使用し、異なる仮想ホスト上のさまざまなサービス用のトラフィックを受け付ける場合があります。この設定を行うには、このマニュアルに記載された方法にしたがって、Gateway アプライアンスのネットワーク設定でこれらのアドレスを指定する必要があります。そのあとポリシーで、追加の IP アドレスにポート定義を関連付けます。ポートの設定については、『*Cisco ACE XML Gateway User Guide*』を参照してください。

Manager の IP アドレス

各 Manager は、1 つのイーサネット ポートおよび 1 つの固定 IP アドレスだけを使用します。複数の物理イーサネット ポートのあるアプライアンス シャーシでは、任意のイーサネット ポートを使用して Manager をネットワークに接続できます。

セキュリティを強化するために、ネットワーク管理者が Manager アプライアンスを専用のファイアウォールの後ろ側に配置する場合もあります。通常、このファイアウォールは DMZ の後ろ側にある企業イントラネットに存在します。この構成では、実稼動 Manager アプライアンスと、エクストラネットから着信するパケットとの間で、最低 3 つのファイアウォール バリアと 1 つの Gateway が配置されることになります。