ネットワークと IP アドレスの割り当て

この付録の構成は、次のとおりです。

イーサネット インターフェイス

Cisco コンテンツ セキュリティ アプライアンスには、構成（任意選択の光ネットワーク インターフェイスがあるかどうか）に応じて、システムの背面パネルに最大4つのイーサネットインターフェイスがあります。次のラベルが付いています。

- 管理
- Data1
- Data2
- Data3
- Data4

IP アドレスとネットマスクの選択

ネットワークを設定するとき、コンテンツ セキュリティ アプライアンスが発信パケットの送信に一意のインターフェイスを選択できる必要があります。この要件によって、イーサネットインターフェイスの IP アドレスとネットマスクの選択に関して、いくつかのことが決まります。単一のネットワークに配置できるインターフェイスは1つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、指定されたネットワークの物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとしていずれか 1 つの IP アドレスを使用して、インターフェイスからパケットを送信できます。このプロパティは、仮想ゲートウェイ テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは IP アドレスの残りのビットです。4 オクテット アドレス内の有効なビット数は、クラスレス ドメイン間ルーティング（CIDR）形式で表現されることがあります。これは、スラッシュ記号、後にビット数（1～32）が続きます。

この方法では、単純にバイナリ表記で 1 を数えることでネットマスクを表現できます。したがって 255.255.255.0 は「/24」となり、255.255.240.0 は「/20 」となります。

インターフェイス設定のサンプル

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。コンテンツ セキュリティ アプライアンスの場合、これらのインターフェイス名は、3 つのインターフェイス（Management、Data1、Data2）の中の 2 つのインターフェイスを示します。

ネットワーク 1：

個別のインターフェイスは別のネットワーク上に存在するように示す必要があります。

インターフェイス	IPアドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.X宛てのデータ（X は自分のアドレスを除く 1 ～ 255 の任意の数字、この場合は 10）は Int1 に出力されます。192.168.0.X 宛てのすべてのデータは Int2 に出力されます。この形式ではない他のアドレス（最も考えられるのは WAN またはインターネット上）に向かうパケットは、デフォルト ゲートウェイに送信されます。デフォルト ゲートウェイはこれらのネットワークのどちらかの上に存在する必要があります。その後、デフォルト ゲートウェイがパケットを転送します。

ネットワーク 2：

2つの異なるインターフェイスのネットワーク アドレス（IPアドレスのネットワーク部分）は同じにすることができません。

イーサネットインターフェイス	IPアドレス	ネットマスク	ネット アドレス
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

これは、2つのイーサネット インターフェイスが同じネットワーク アドレスを持つという、競合した状態を表しています。コンテンツ セキュリティ アプライアンスからのパケットが

192.168.1.11 に送信された場合、パケットの配信にどのイーサネット インターフェイスを使用すべきかは特定できません。2 つのイーサネット インターフェイスが 2 つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。コンテンツ セキュリティ アプライアンスでは、競合するネットワークを設定できません。

2 つのイーサネット インターフェイスを同じ物理ネットワークに接続することはできますが、コンテンツ セキュリティ アプライアンスが一意の配信インターフェイスを選択できるように IP アドレスとネットマスクを設定する必要があります。

IP アドレス、インターフェイス、およびルーティング

GUI または CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルト ゲートウェイ）が選択した内容よりも優先されます。

たとえば、次のように 3 つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定されたコンテンツ セキュリティ アプライアンスがあるとします（すべて /24 と仮定）。

イーサネット	IP
管理	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

デフォルト ゲートウェイは 192.19.0.1 です。

ここで、AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、Data1 上の IP（192.19.1.100）を選択した場合、すべての TCP トラフィックが Data1 イーサネット インターフェイス経由になると予想されることと思います。しかし、実際には、デフォルト ゲートウェイとして設定されているインターフェイス（ここでは Management）からトラフィックが送出されます。ただし、トラフィックの送信元アドレスには Data1 の IP が設定されています。

要約

コンテンツ セキュリティ アプライアンスは、配信可能なパケットが経由する一意のインターフェイスを常に識別できなければなりません。この決定を行うために、コンテンツ セキュリティ アプライアンスは、パケットの宛先 IP アドレスと、そのイーサネット インターフェイスのネットワークおよび IP アドレス設定を組み合わせて使用します。次の表に、ここまで説明してきた例をまとめます。

	同じネットワーク	異なるネットワーク
同じ物理インターフェイス	許可	許可
異なる物理インターフェイス	不可	許可

コンテンツセキュリティアプライアンスを接続するための戦略

アプライアンスを接続する際には、次の点に留意してください。

- 通常、管理トラフィック（CLI、Web インターフェイス、ログ配信）は、電子メール トラフィックよりもはるかに少量です。
- 2 つのイーサネット インターフェイスが同じネットワーク スイッチに接続されているが最終的にダウンストリームの別のホスト上の単一インターフェイスと通信するだけの場合、あるいはすべてのデータがすべてのポートにエコーされるネットワーク ハブにそれらが接続されている場合、2 つのインターフェイスを使用しても得られる利点はありません。
- 1000Base-T で動作しているインターフェイスでの SMTP カンバセーションは、100Base-T で動作している同じインターフェイスでのカンバセーションよりも少し高速ですが、速くなるのは理想的な条件下でのみです。
- 配信ネットワークのその他の部分にボトルネックがある場合、ネットワークへの接続を最適化しても意味がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続に使用するインターフェイスの数とそれらへのアドレス指定の方法は、基礎となるネットワークの複雑性によって決める必要があります。ご使用のネットワーク トポロジやデータのボリュームから判断して不要であれば、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。