CHAPTER 3

VLAN 構成のプランニング

ポートを ASA 5505 上の論理 VLAN にグループ化すると、大規模なプライベート ネットワークをセグメント化でき、サーバ、企業のコンピュータ、および IP 電話などのリソースに対応している可能性がある重要なネットワーク セグメントの保護を強化できます。

この章では、VLAN 構成における ASA 5505 の構成オプションと、必要な VLAN の数を判別する方法を説明します。各 VLAN にポートを割り当てる方法についても説明します。

この章には、次の項があります。

ASA 5505 上の VLAN について

ネットワーク内に ASA 5505 を構成する方法を決定したら、その構成をサポートするのに必要な VLAN の数と、各 VLAN に割り当てるポートの数を決定する必要があります。

この項では、それらを決定できるよう、ASA 5505 上の VLAN がどのように機能するかを説明します。

この項は、次の内容で構成されています。

ASA 5505 上の物理ポートについて

ASA 5505 には、スイッチ ポートと呼ばれる 8 つの Fast Ethernet ポートを備えた内蔵スイッチがあります。8 つの物理ポートのうち 2 つは、Power Over Ethernet（PoE）ポートです。PoE ポートには、PC、IP 電話、DSL モデムなどのユーザ装置を直接接続できます。別のスイッチに接続することもできます。詳細については、P.4-11 の「ポートおよび LED」を参照してください。

VLAN について

8 つの物理ポートを、別個のネットワークとして機能する VLAN と呼ばれるグループに分割できます。これによって、企業のセキュリティを向上させることができます。異なる VLAN にあるデバイスは、適切なセキュリティ ポリシーが適用されている適応型セキュリティ アプライアンスを使用してトラフィックを通すことによってのみ、互いに通信できるからです。

ASA 5505 には、VLAN1 と VLAN2 の 2 つの VLAN が事前設定されています。デフォルトでは、イーサネット スイッチ ポート 0/0 は VLAN2 に割り当てられています。他のすべてのスイッチ ポートは、デフォルトで VLAN1 に割り当てられています。

同じ VLAN 上の物理ポートは、ハードウェア スイッチングを使用して互いに通信できます。VLAN は、ルートとブリッジを使用して相互に通信します。たとえば、VLAN1 上のスイッチ ポートが VLAN2 上のスイッチ ポートと通信を行うとき、適応型セキュリティ アプライアンスは設定されているセキュリティ ポリシーをトラフィックに適用し、2 つの VLAN 間でトラフィックをルートまたはブリッジします。

厳密なアクセス コントロールを課して機密デバイスを保護するため、VLAN 間の通信を制限するセキュリティ ポリシーを VLAN に適用できます。セキュリティ ポリシーを個々のポートに適用することもできます。たとえば、同じ VLAN 上に 2 つのポートがあり、互いに通信するのを望まない複数のデバイスが接続されている場合、ポート レベルでセキュリティ ポリシーを適用することができます。

ASA 5505 上のスイッチ ポートは、VLAN に割り当ててからでなければイネーブルにすることはできません。Base プラットフォームでは、各スイッチ ポートを同時に 1 つの VLAN だけに割り当てることができます。Security Plus ライセンスでは、1 つのポートを使用して外部スイッチ上の 3 つの VLAN 間をトランキングし、組織が大きくなった場合に構成を拡張することができます。

VLAN を作成してポートを割り当てるには、次の方法があります。

VLAN の設定方法	参照先
ASDM Startup Wizard	第 5 章「適応型セキュリティ アプライアンスの設定」
ASDM GUI を使用した設定	ASDM オンライン ヘルプ
コマンドライン インターフェイス	*Cisco Security Appliance Command Reference*

VLAN の最大数とタイプ

使用しているライセンスに応じて、ASA 5505 でアクティブにできる VLAN の数が決まります。

ASA 5505 には 2 つの VLAN が事前設定されていますが、使用しているライセンスに応じて最大 3 つの VLAN を作成できます。たとえば、内部、外部、および DMZ ネットワーク セグメント用の VLAN を作成できます。各アクセス スイッチ ポートは、1 つの VLAN に割り当てられます。トランク スイッチ ポートは、複数の VLAN に割り当てることができます。

Base プラットフォームでは、DMZ VLAN と内部 VLAN 間の通信が制限されています。内部 VLAN は DMZ VLAN にトラフィックを送信できますが、DMZ VLAN は内部 VLAN へのトラフィック送信を許可されていません。

Security Plus ライセンスにはこの制限がなく、完全な DMZ 構成を可能にしています。

表 3-1 に、各ライセンスでサポートされている接続数と接続タイプを示します。

表 3-1　アクティブ VLAN のライセンス制限

ライセンス タイプ	モード	接続数
Base プラットフォーム	透過モード	最大 2 つのアクティブ VLAN。
	ルーテッド モード	最大 3 つのアクティブ VLAN。DMZ VLAN から内部 VLAN へのトラフィックの開始は制限されています。
Security Plus ライセンス	透過モード	最大 3 つのアクティブ VLAN。1 つはフェールオーバー用にする必要があります。
	ルーテッド モード	最大 20 のアクティブ VLAN（通常のトラフィック用）。 1 つのアクティブ VLAN（フェールオーバー用）。 ISP に対するバックアップ リンクとしての 1 つのアクティブ VLAN。バックアップ インターフェイスは、プライマリ インターフェイスへのルートが失敗しない限り、トラフィックを送受信しません。

（注） ASA 5505 適応型セキュリティ アプライアンスは、アクティブおよびスタンバイ フェールオーバーをサポートしていますが、ステートフル フェールオーバーはサポートしていません。

VLAN を使用した構成シナリオ

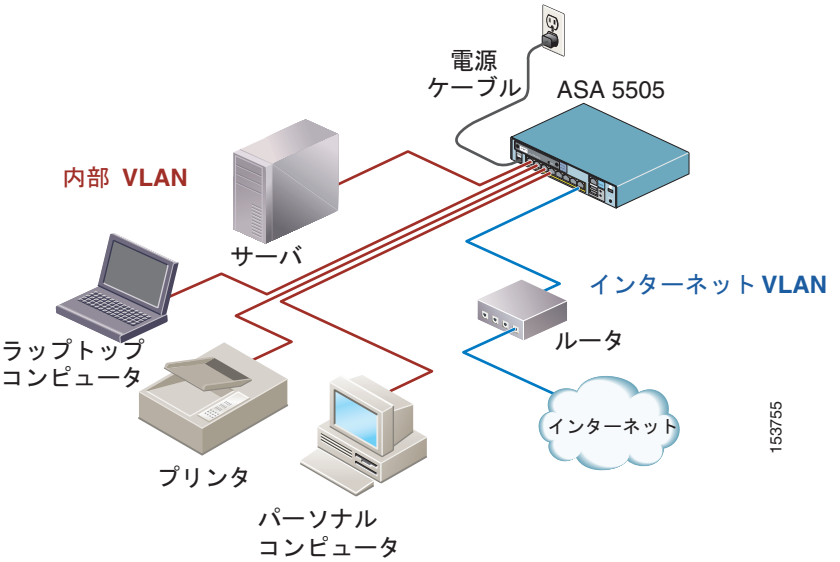
必要な VLAN の数は、適応型セキュリティ アプライアンスにインストールするネットワークの複雑さによって異なります。この項のシナリオをガイドとして使用し、必要な VLAN の数と、それぞれの VLAN に割り当てるポートの数を判別することができます。

この項は、次の内容で構成されています。

2 つの VLAN を使用した基本的な構成

ほとんどの構成では、図 3-1 に示すように、内部 VLAN と外部 VLAN の 2 つの VLAN のみを作成する必要があります。

図 3-1　　2 つの VLAN を使用した構成



この例では、ネットワークに内部 VLAN と外部 VLAN が含まれます。内部 VLAN は、互いに通信を行うことを VLAN 内のすべてのデバイスに許可し、外部 VLAN は、インターネット上のデバイスとの通信をユーザに許可します。

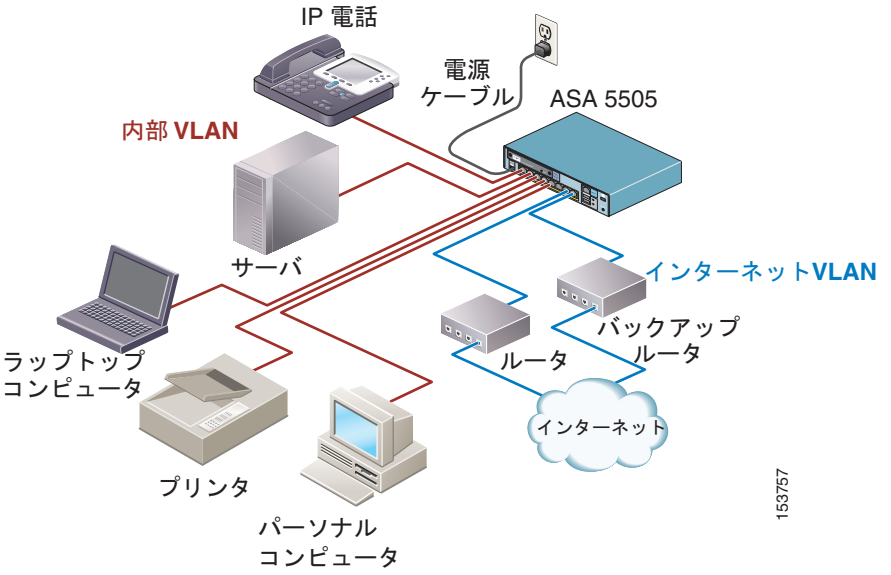
内部 VLAN は、デスクトップ コンピュータ、ネットワーク プリンタ、および他のデバイスを接続する最大 7 つの物理ポートで構成できます。このシナリオでは、外部 VLAN は、外部 WAN ルータを使用するシングル ISP 接続で構成されます。

図 3-1 では、内部 VLAN は ASA 5505 の スイッチ ポートを 4 つ使用し、外部 VLAN は 1 つだけ使用しています。3 つのスイッチ ポートが未使用です。

（注） この構成は PIX 501 を使用するセキュリティ構成に類似しています。ファイアウォールの背後にあるデバイスが内部および外部で通信できる PIX 501 セキュリティ アプライアンスを使用したセキュリティ構成をすでに使用している場合は、同じ構成をそのまま使用し、PIX 501 デバイスを ASA 5505 デバイスに交換できます。

この同じカスタマーが 2 つのインターネット接続を必要とする場合は、図 3-2 に示すように、外部 VLAN に追加ポートを割り当てることができます。この構成には、内部 VLAN と外部 VLAN が含まれます。外部 VLAN には、一方の接続が切断されたときにリンク冗長性を提供する2つの外部接続が使用されています。

図 3-2　デュアル ISP 接続を使用した内部 VLAN

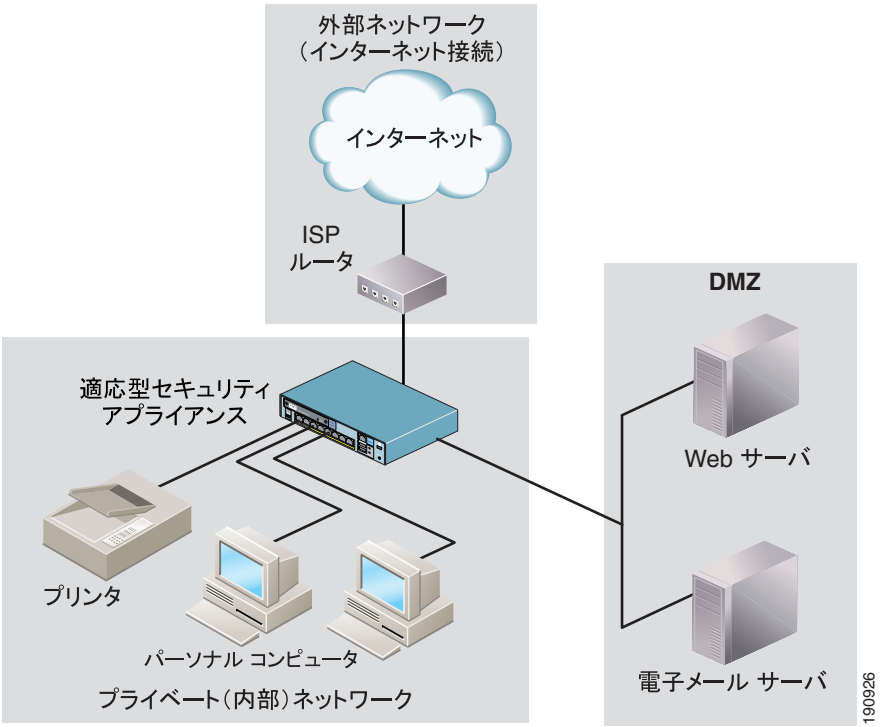


非常に複雑なネットワークの場合でも、内部用と外部用の 2 つの VLAN だけを使用して構成することができます。

DMZ 構成

3 つの VLAN を必要とする唯一の構成は、内部ネットワークだけでなく DMZ を保護する必要がある構成です。構成に DMZ がある場合、DMZ は固有の VLAN 上にある必要があります。

図 3-3　　3 つの VLAN を必要とする構成



この例では、3 つの物理スイッチ ポートが内部 VLAN に割り当てられ、2 つのスイッチ ポートが DMZ VLAN に割り当てられ、1 つのスイッチ ポートが外部 VLAN に割り当てられています。2 つのスイッチ ポートが未使用です。

3 つの VLAN を使用したテレワーカー構成

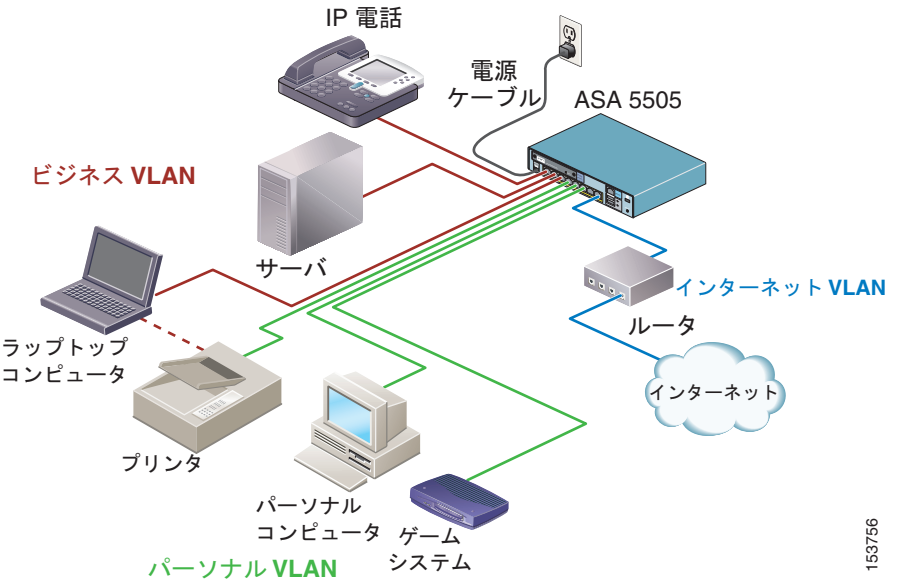
3 つの VLAN の使用は必須ではありませんが、テレワーカーをサポートするためにリモート VPN ハードウェア クライアントを構成する状況などでは、役立つことがあります。

図 3-4 では、ASA 5505 をホーム オフィス環境に設置しており、リモート VPN ハードウェア クライアントとして使用しています。ASA 5505 は、次の 3 つの VLAN に対して設定されています。

- メインの企業ネットワークへのアクセスをサポートするすべてのデバイスで構成されている内部（ワーク）VLAN
- 家族の全員が使用できるデバイスで構成されている DMZ（ホーム）VLAN
- 内部 VLAN と DMZ VLAN の両方にインターネット接続を提供する外部（インターネット）VLAN

この場合、ASA 5505 が内部（ワーク）VLAN 上の重要なアセットを保護するため、これらのデバイスが DMZ（ホーム）VLAN からのトラフィックの影響を受けることはありません。内部（ワーク）VLAN 内のデバイスと企業のヘッドエンド デバイスとの安全な接続を確立するには、Easy VPN ハードウェア クライアント機能をイネーブルにし、内部（ワーク）VLAN からのトラフィックだけが Easy VPN 接続を開始するようにします。この構成では、DMZ（ホーム）VLAN のユーザは内部（ワーク）VLAN とは無関係にインターネットを閲覧でき、内部（ワーク）VLAN のセキュリティが損なわれることはありません。

図 3-4　3 つの VLAN を使用したテレワーカー構成



この例では、ASA 5505 の物理ポートが次のように使用されています。

- 3 つの物理スイッチ ポートで構成される内部（ワーク）VLAN。そのうちの 1 つは Power over Ethernet（PoE）スイッチ ポートで、IP 電話に使用します。
- 3 つの物理スイッチ ポートで構成される DMZ（内部）VLAN。
- 1 つの物理スイッチ ポートで構成される外部（インターネット）VLAN。この物理スイッチ ポートは、外部 WAN ルータまたはブロードバンド モデムを使用するシングル ISP 接続をサポートしています。

プリンタは、内部 VLAN と DMZ VLAN の両方で共有されます。

VLAN の詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

次の作業

第 4 章「ASA 5505 の取り付け」に進みます。

次の作業