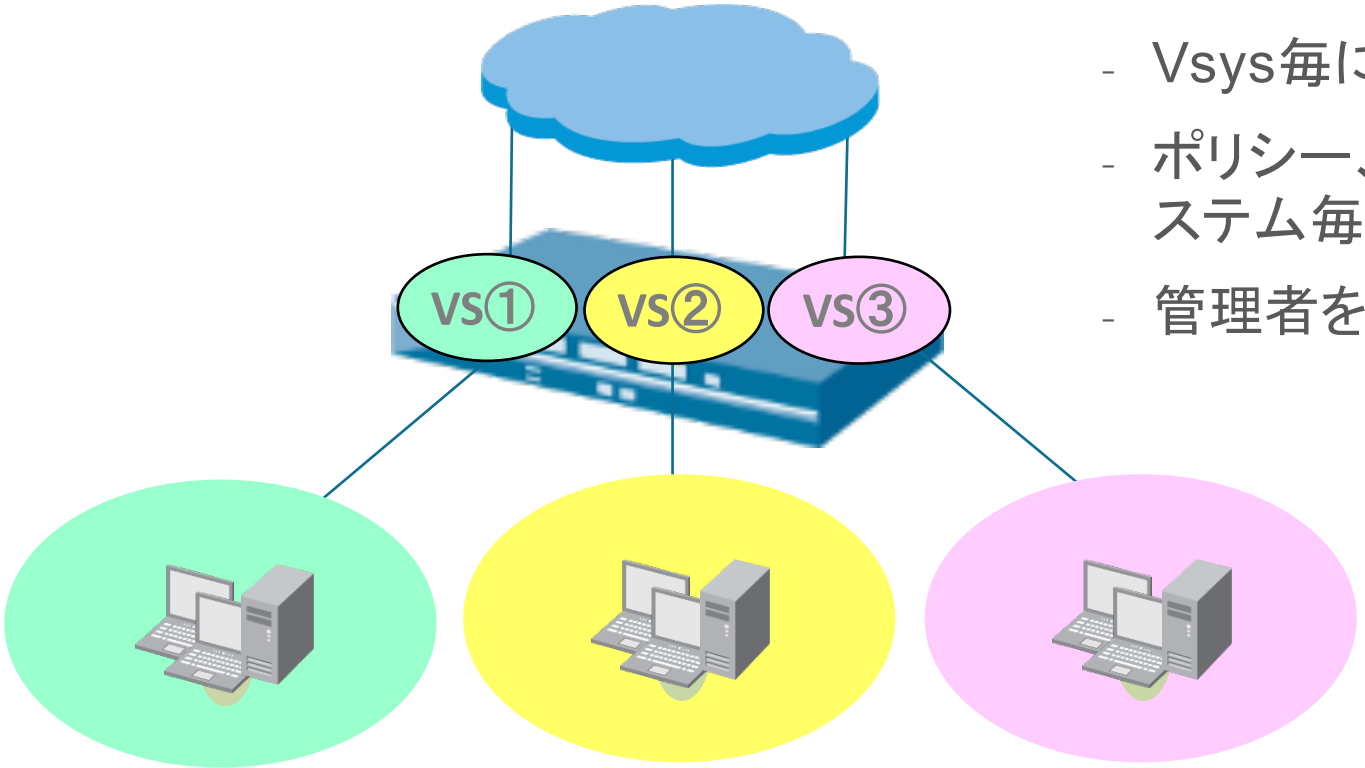
PALO ALTO NETWORKS

Virtual System(仮想システム)と内部通信について

May.2016

***Virtual System*(仮想システム)とは**

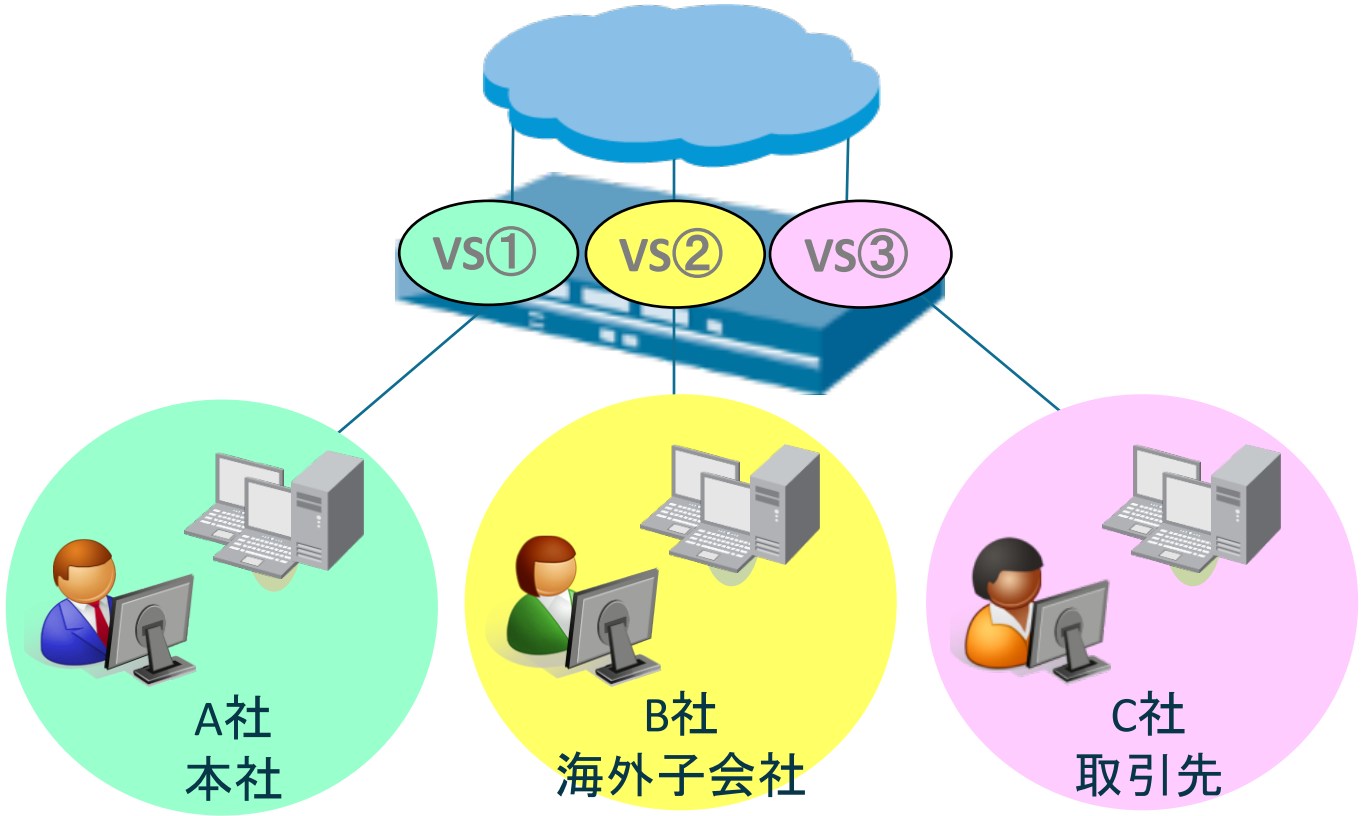
- 物理的に1台(冗長構成であれば2台)のPAシリーズを論理的に独立した複数のファイアウォールとして動作
  - 1台のファイアウォールを複数の顧客や部門で共有することで、少ない投資で効率の高いシステムを構成することが可能



- Vsys毎に個別に設計が必要
- ポリシー、レポート、ログを仮想システム毎に保持
- 管理者を分けての運用が可能

Virtual System *利用イメージ*

- A社： A社のファイアウォールの運用管理
- B社： B社のファイアウォールを運用管理
- C社： C社のファイアウォールを運用管理



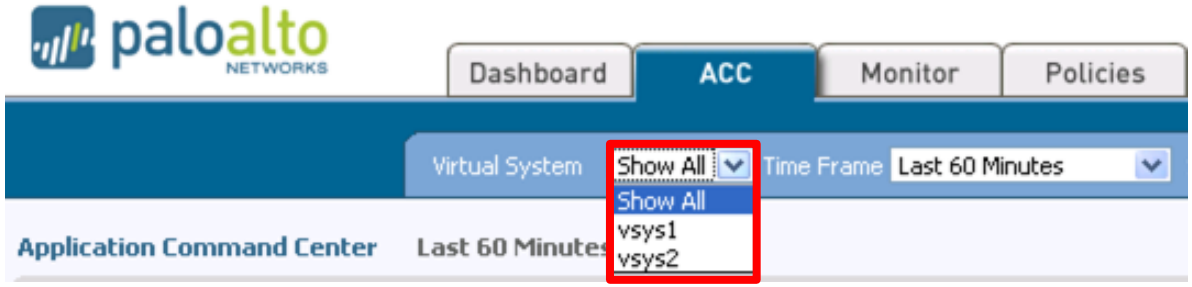
Virtual System 概要

- 各Virtual System毎に、インターフェースを定義、ネットワーク設定、およびセキュリティポリシーを作成・閲覧が可能
  - 各Virtual Systemsでは、物理的および論理的なインタフェース（VLAN やvirtual wireを含む）、仮想ルータ、セキュリティゾーンを指定
  - 各Virtual Systemsでは通常のシステムと同様に、個別でアドレスやサービスといったオブジェクトを定義して専用のセキュリティポリシーを定義
  - 各Virtual Systems毎でACCやログ、レポートも個別で閲覧可能
  - 特定の仮想システムの管理やログ閲覧のみが可能な管理者アカウントを作成し、管理権限を委譲することが出来、またsyslogやSNMPの設定も各Virtual Systems毎で個別定義が可能

Virtual System 設定例

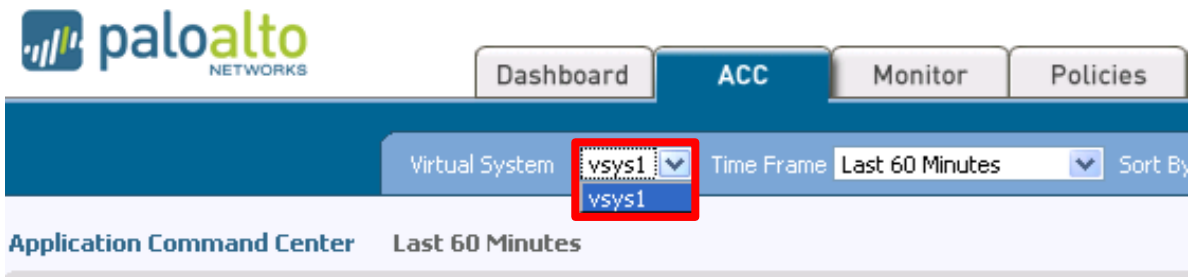
- Super User権限の管理者は、各Virtual Systemの情報を切り替えて閲覧・編集することが可能

SuperUser権限のACC画面



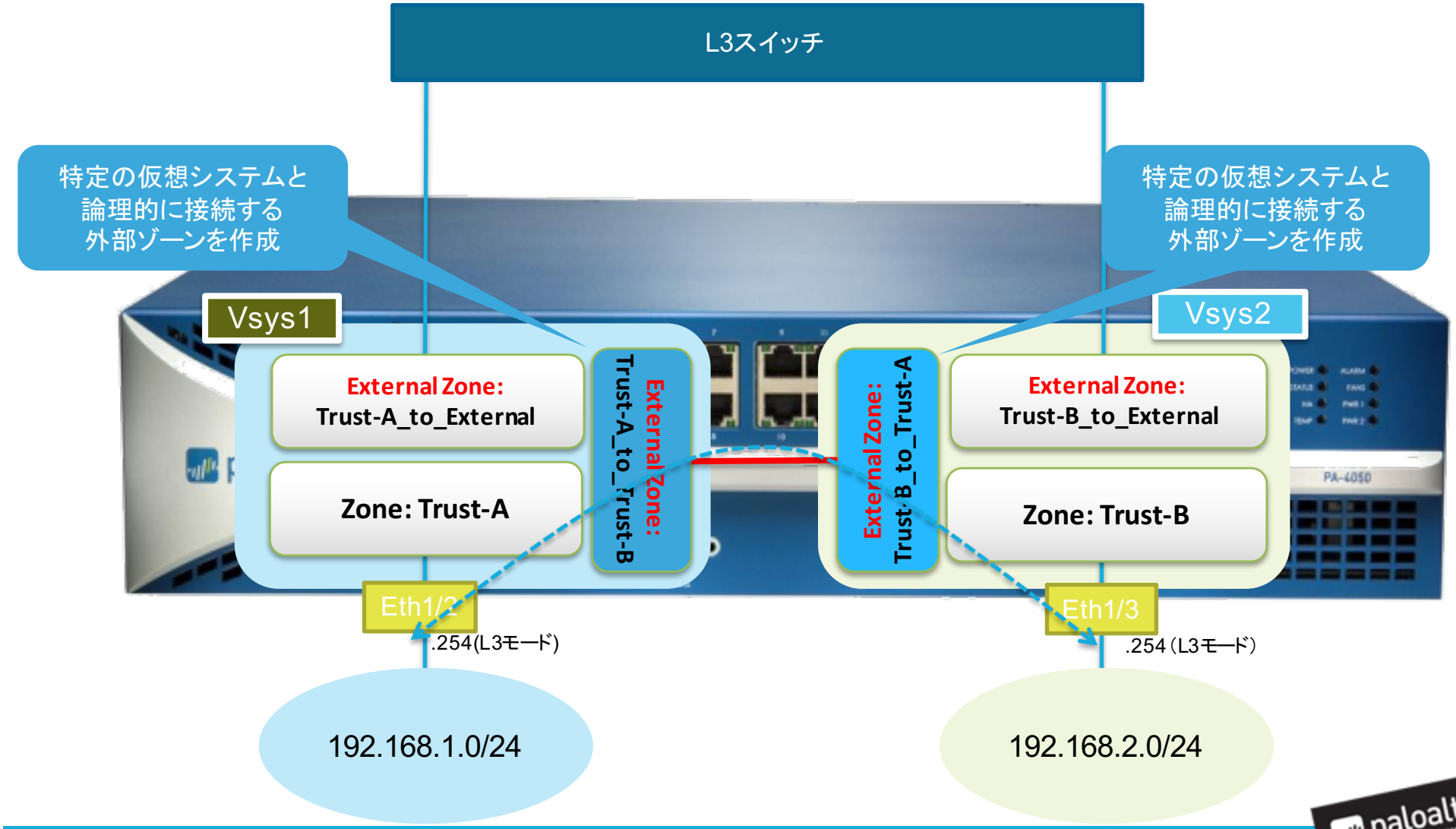
- 各Virtual Systemの管理者は自分のVirtual Systemの設定　（オブジェクトやポリシー）のみを閲覧・編集することが可能

Virtual Systemsys admin権限でのACC画面



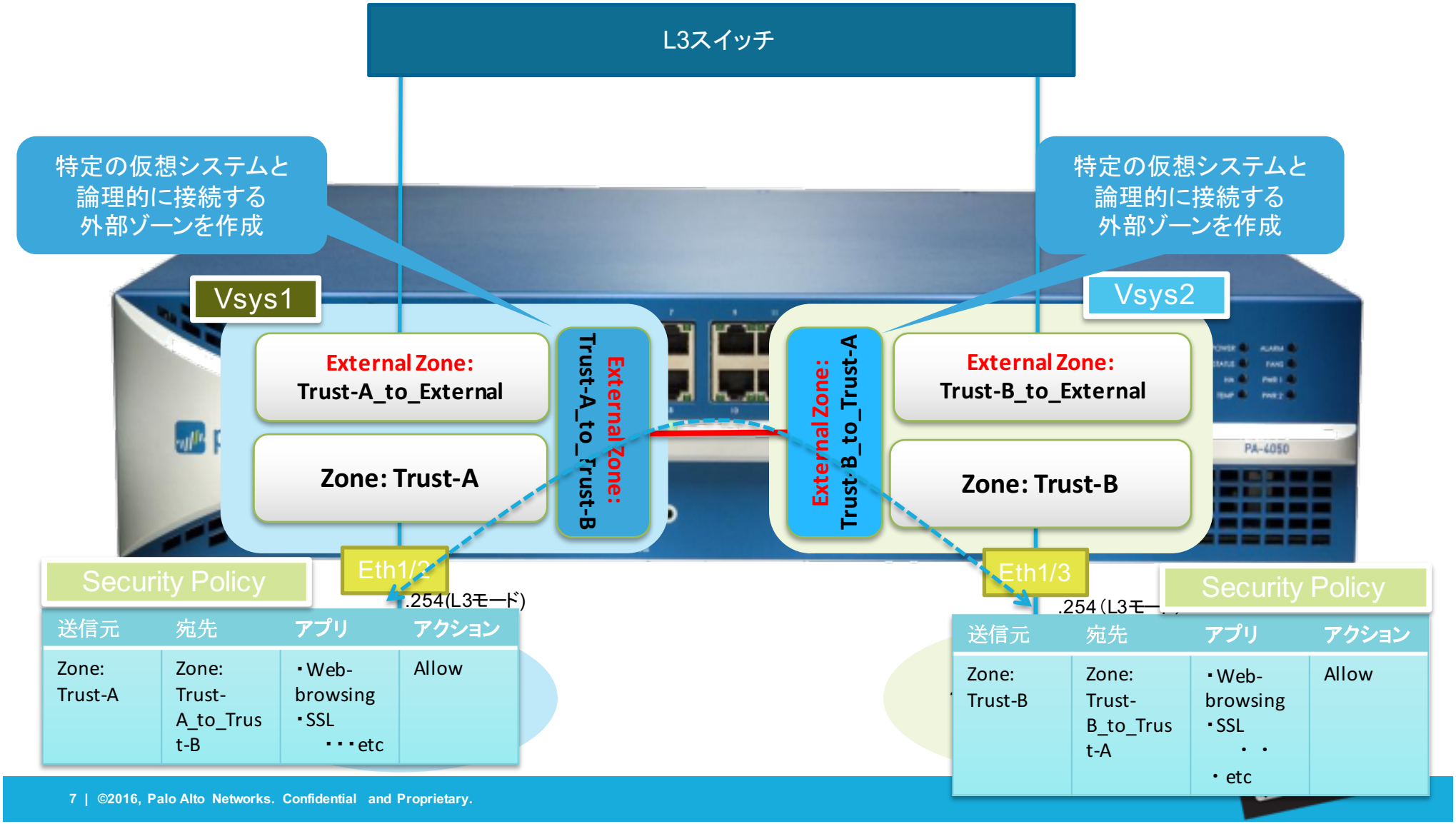
内部Virtual System間通信の許可

- 内部の複数VSYS間の通信を許可することも可能です。この場合相互に論理的に接続する外部ゾーンを設定します。



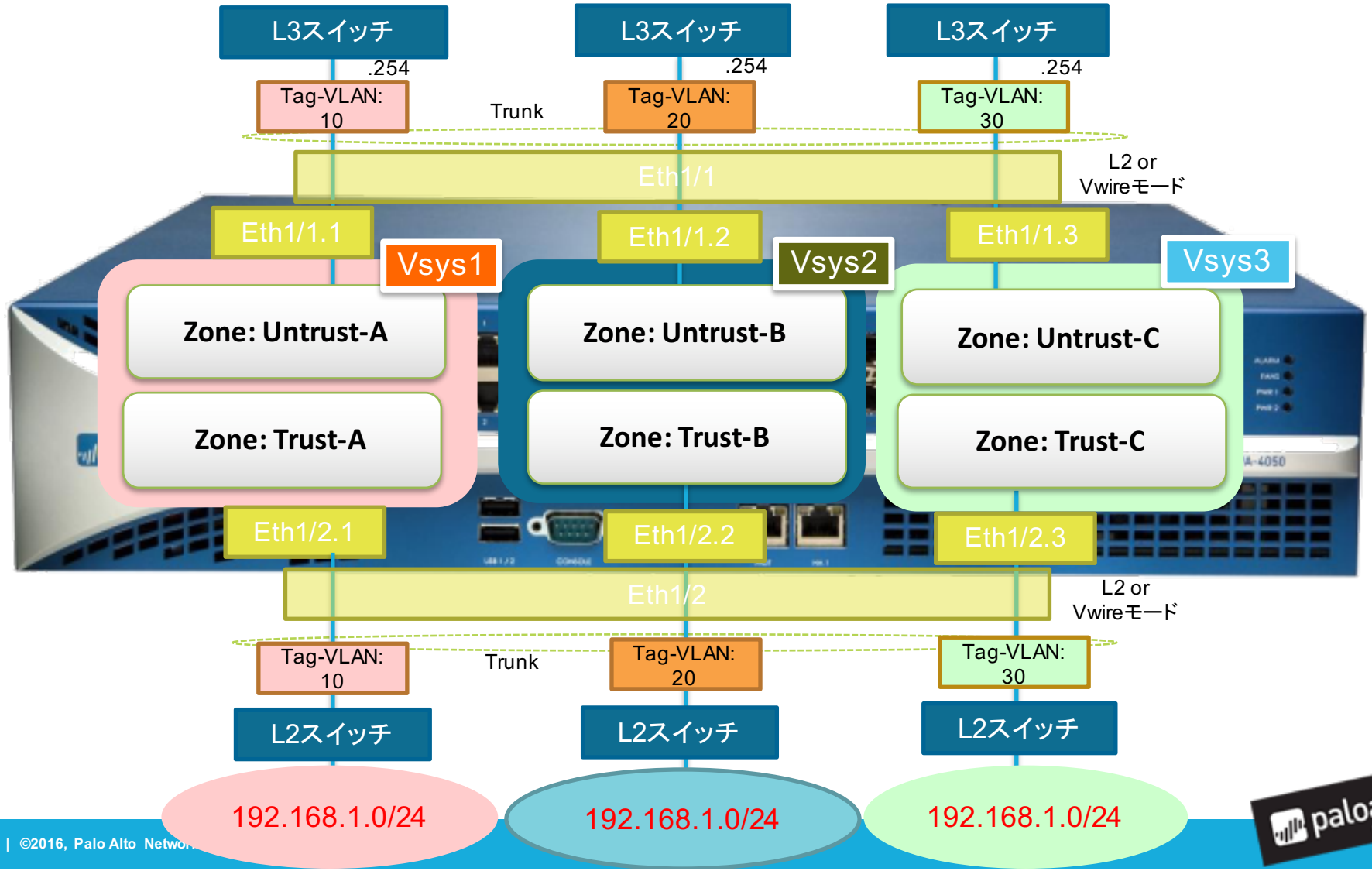
内部Virtual System間通信の許可

- 具体的な設定イメージ:



制限①：IPアドレスレンジの重複について

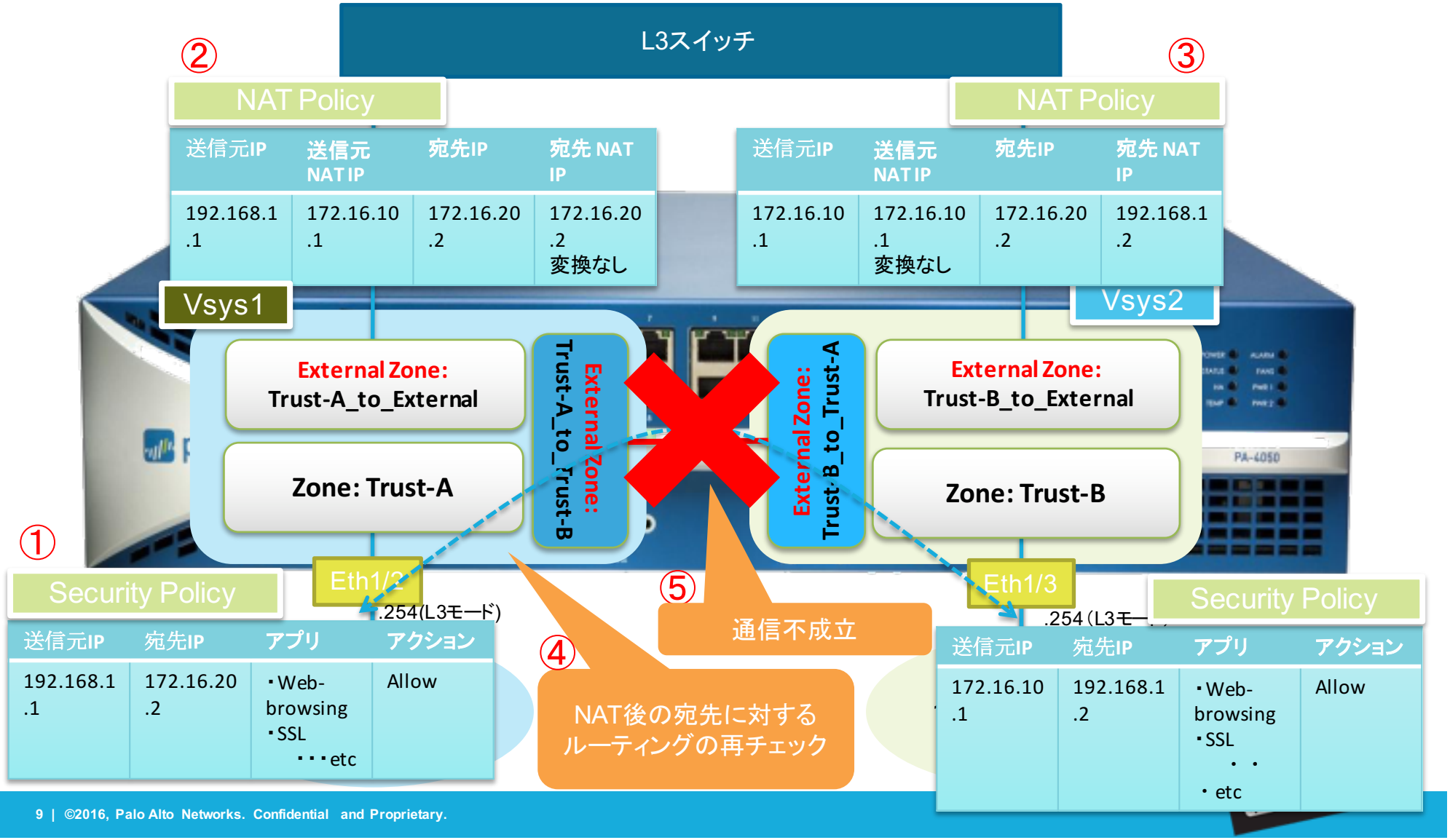
- Virtual System間で収容するIPアドレスレンジの重複が許容されており、更に別々のポリシーで通信制御を行うことも可能
- 但し、L3モードで収容する場合は同一筐体上のインターフェイス/Virtual Routerに重複するIPアドレスを設定することは不可



制限②：内部Virtual System間通信の制限

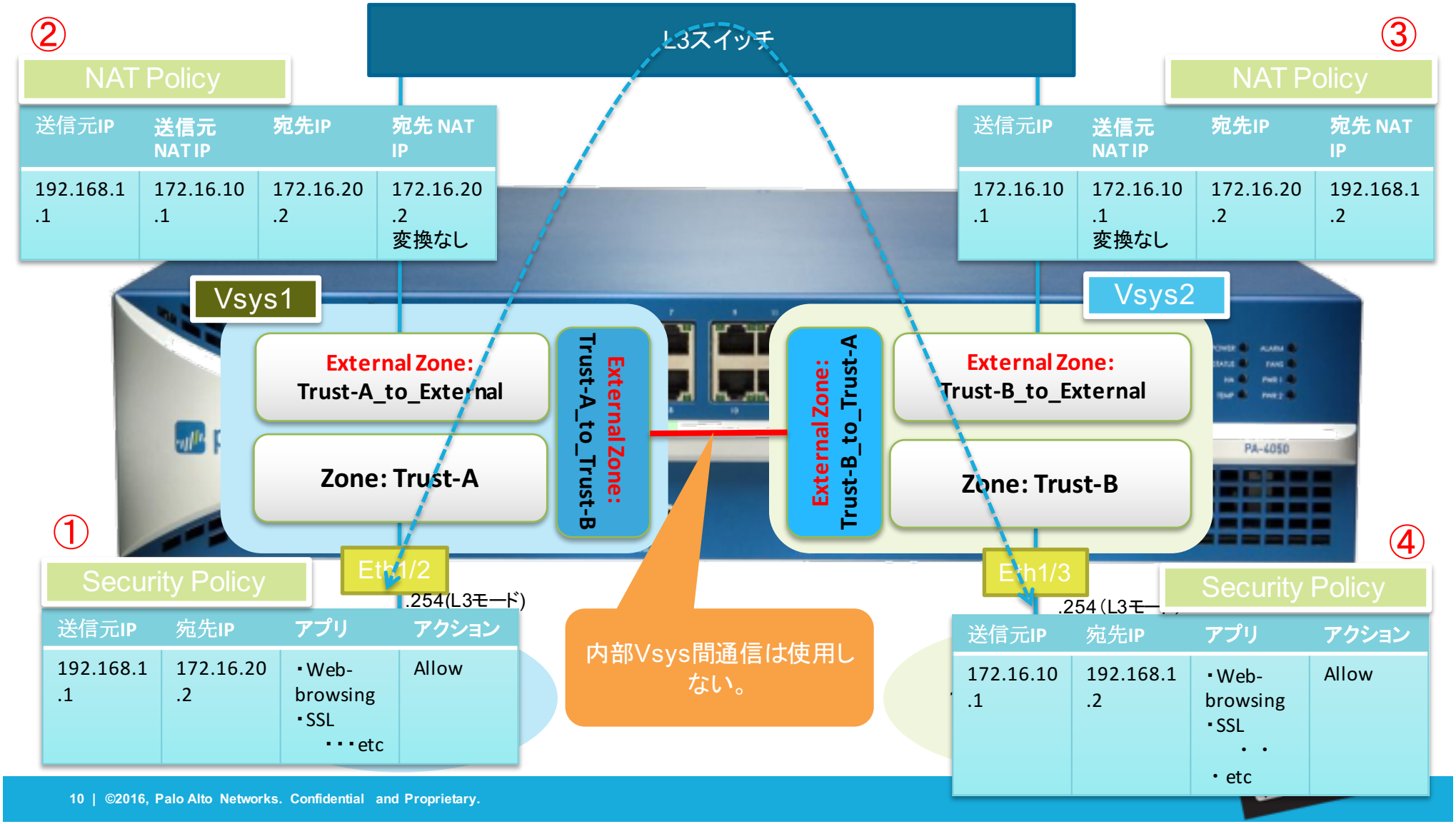
- Vsys1およびVsys2ともに管理セグメントに同一ネットワーク（下記の例では、192.168.1.0/24）が重複していると、この間の通信は成立しません。

※ NAT変換後の宛先アドレスをパケットが入ってきた元のVsysに再確認するため。



内部セグメントが重複する通信（制限②）の回避方法

- 内部Vsys間通信でのルーティングは行わず、外部のルータ機能（L3スイッチ等）を経由することによって、NATを利用した同じセグメント間の通信を実現できる。




paloalto
NETWORKS®