The Guaranteed Network
いちばん近くで、もっと先へ。

AX＆パロアルトネットワークス PA シリーズ
セキュア仮想ネットワークソリューション
システム構築ガイド

初 版

資料 No. NTS-12-R-039

アラクサラネットワークス株式会社

はじめに

セキュア仮想ネットワークソリューションは、アラクサラ AX シリーズによるネットワークパーティションと、仮想ファイアウォール機能を持つ機器とを組合せて構築する、高度なセキュリティ管理を実現するソリューションです。本ガイドは、仮想ファイアウォールにパロアルトネットワークス社の PA シリーズを用いた場合における、セキュア仮想ネットワークソリューションの一例を紹介し、また同システム構築の一助となることを目的としています。

関連資料

・AX シリーズ ネットワークパーティション ソリューションガイド［基本編］［認証編］［応用編］
・AXシリーズ製品マニュアル（ http://www.alaxala.com/jp/techinfo/manual/index.html ）

・パロアルトネットワークス (http://www.paloaltonetworks.jp/)
・Palo Alto Networks (http://www.paloaltonetworks.com/) (英文サイト)

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。弊社製品を用いたシステム構築の一助としていただくためのものとご理解いただけますようお願いいたします。

本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX シリーズ

AX6600S	Ver. 11.7
AX3650S	Ver. 11.9
AX2530S	Ver. 3.3
AX1200S	Ver. 2.4

パロアルトネットワークス PA シリーズ

PAN-OS™	Release 4.1.6

なお本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

AX シリーズに関し、本製品を輸出される場合には、外国為替および外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。なお不明な場合は、弊社担当営業にお問い合わせ下さい。

商標一覧

・アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
・Palo Alto Networks Logo, Panorama は米国 Palo Alto Networks, inc.の商標および登録商標です。
・Ethernet およびイーサネットは、富士ゼロックス(株)の登録商標です。
・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

目次

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

1. 仮想ネットワークによるセキュリティレベルの向上

1.1 重要度を増すシステムのセキュリティ対策

近年、企業の持つ個人情報や機密情報等の漏洩からその個人ないし企業に莫大な損害が発生したり、国家の機密情報の漏洩が世界的な社会問題になったりするなど、企業や行政団体、教育機関など社会組織において各種情報の取り扱いが厳しくなっています。

また、情報管理のためのツールであるITシステムにおいては、これまで危機管理として、業務に使うPCへのウイルス感染やスパムメール、インターネットからの攻撃など、システム外部からの要因に対しシステム内の情報を守ることが一般的でした。

しかしこの数年において

- クラウドのビジネス利用による情報管理そのもののアウトソース化 (情報が外部にある)
- ノート型 PC に加えタブレット端末やスマートフォンなど個人向け多機能端末の爆発的な普及
- BYOD など公的/私用の境界のない機器利用形態の提案
- ソーシャルメディア(Facebook, Twitter など)の一般化による個人の不特定多数への発言機会増加

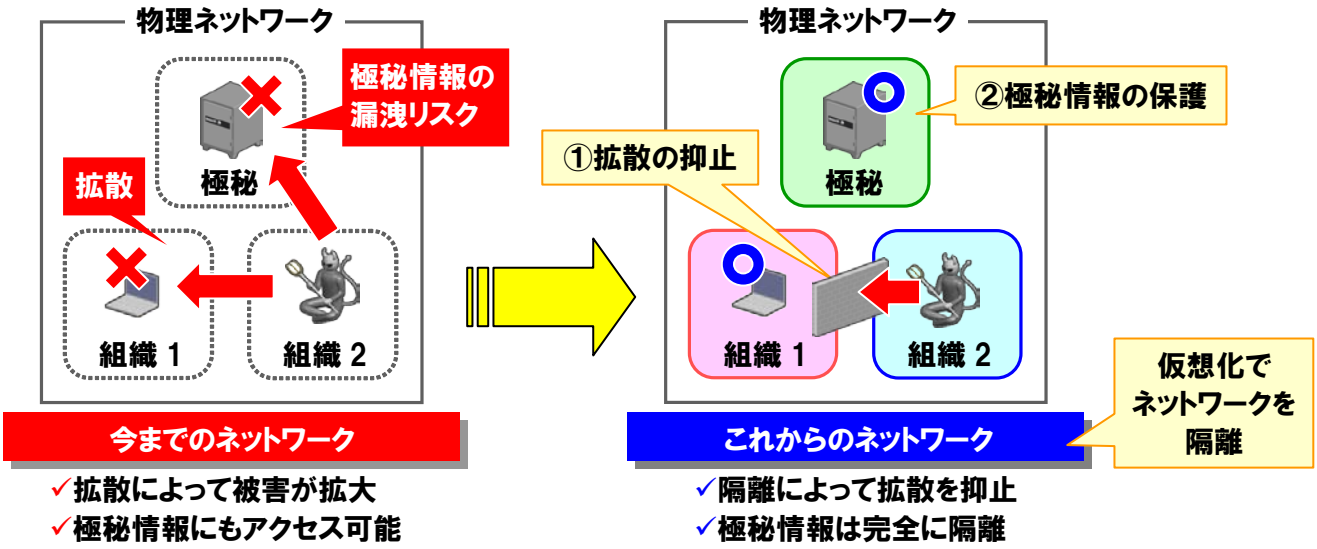
以上のようにシステム全体をとりまく環境が大きく変化しており、このために

- 組織内に持ち込まれたデバイスからのウイルス感染またはマルウェアによる情報漏洩
- (不意にせよ意図的であるにせよ)個人の SNS などへの機密情報に関することの発言
- 悪意を持つユーザの組織内部からの意図的な攻撃や機密情報の漏洩操作

など、守るべき情報に対する脅威の内容も高度かつ多種にわたるようになってきました。

このような背景から、これからのITシステムにおいては、組織内の各部門で持つさまざまな情報に対し、その情報をアクセスすべき権限を持つユーザーにのみ適切なアクセス権限を与え、その情報に直接関係しないユーザには不必要にアクセスさせないような環境を作る必要があります。また万が一情報が漏洩した際も被害を最小限に食い止められるよう、サーバやネットワーク等、情報の管理単位を部門毎に細分化することも有効な手段の一つといえます。

つまり、これからの IT システムにおけるセキュリティ管理は、会社、行政団体、教育機関などといった大きな単位から、部門や省庁、学部といった、より細かい単位でのセキュリティ(脅威)管理が重要となるでしょう。



Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

1.2 システムに求められる課題と 2 つの「仮想化」がもたらす解決策

情報を組織毎に細分化し、適切なアクセス権限を与え、状況を監視するには、以下の施策が考えられます。

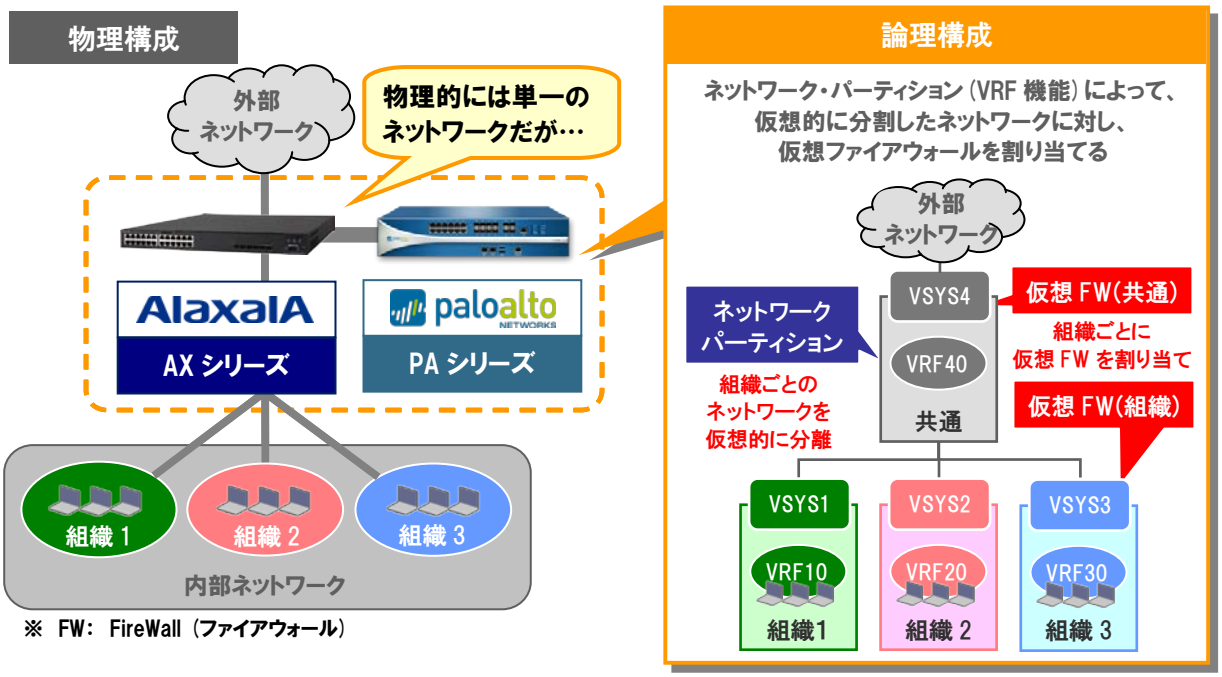
- **ネットワークの分離**
  ネットワークを組織単位で完全に分ける（物理的にアクセスできないようにする）。
- **ユーザ認証**
  認証機能を取り入れることで、不正なユーザを排除。
- **アクセス制御**
  URL、アプリケーションフィルタ等で必要な通信の許可、不要な通信の禁止を制御。
- **アクセスログの記録**
  サーバ、ネットワーク等への不正アクセス等を監視。

セキュリティをより効果的なものとするには、システムと運用の両面から複数の対策を実施する必要があります。しかし以上のような施策を導入する場合、システムにおいてはネットワーク機器装置の増加や、それに伴う各種設定(フィルタ等)の追加が必要です。また運用においては運用・管理の煩雑化など初期投資や運用のためのコストが増加します。これらが大きな阻害要因となり現実にはなかなか導入に至らないケースが多いかと考えられます。

「ネットワークやアクセス制御は組織毎に細分化してセキュリティを強化したいが、それに伴う装置や運用の増加にかかるコストは抑えたい」－これらの相反する課題を解決するソリューションが、以下に示す 2 つの仮想化技術の組み合わせによるソリューションです。

- **ネットワークの仮想化**
  単一の物理ネットワークを複数の仮想ネットワークに分離することで組織間の独立性およびセキュリティの確保が可能となります。
- **ファイアウォールの仮想化**
  仮想ネットワークごとに仮想ファイアウォールを割り当てることで組織単位に最適なセキュリティポリシーを運用します。

このソリューションをより現実的なものとするため、アラクサラネットワークスのネットワーク・パーティションとパロアルトネットワークスの仮想システム(VSYS)を組み合わせることにより「セキュア仮想ネットワークソリューション」を実現しました。セキュア仮想ネットワークソリューションを導入することで、管理単位を細分化した高度なセキュリティを持つシステムを、初期投資・運用・管理のコストを抑えながら実現することができます。



Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

1.3 セキュア仮想ネットワークソリューション概要

セキュア仮想ネットワークソリューションとは、2 つの仮想化技術の組み合わせによって、組織ごとに高度にセキュリティ管理されたネットワークシステムを必要最小限の機器で提供するソリューションです。

2 つの仮想化をどのように組み合わせて実現するのか、それぞれの仮想化の概念を踏まえながら、セキュア仮想ネットワークソリューションの概要を紹介します。

1.3.1 ネットワークの仮想化

組織間のセキュリティを確保するためには、それぞれの組織で独立したネットワークとしてしまうことが最もシンプルかつ簡単な方法です。そこでアラクサラのネットワーク・パーティションで組織ごとに独立したネットワーク構成を作ります。

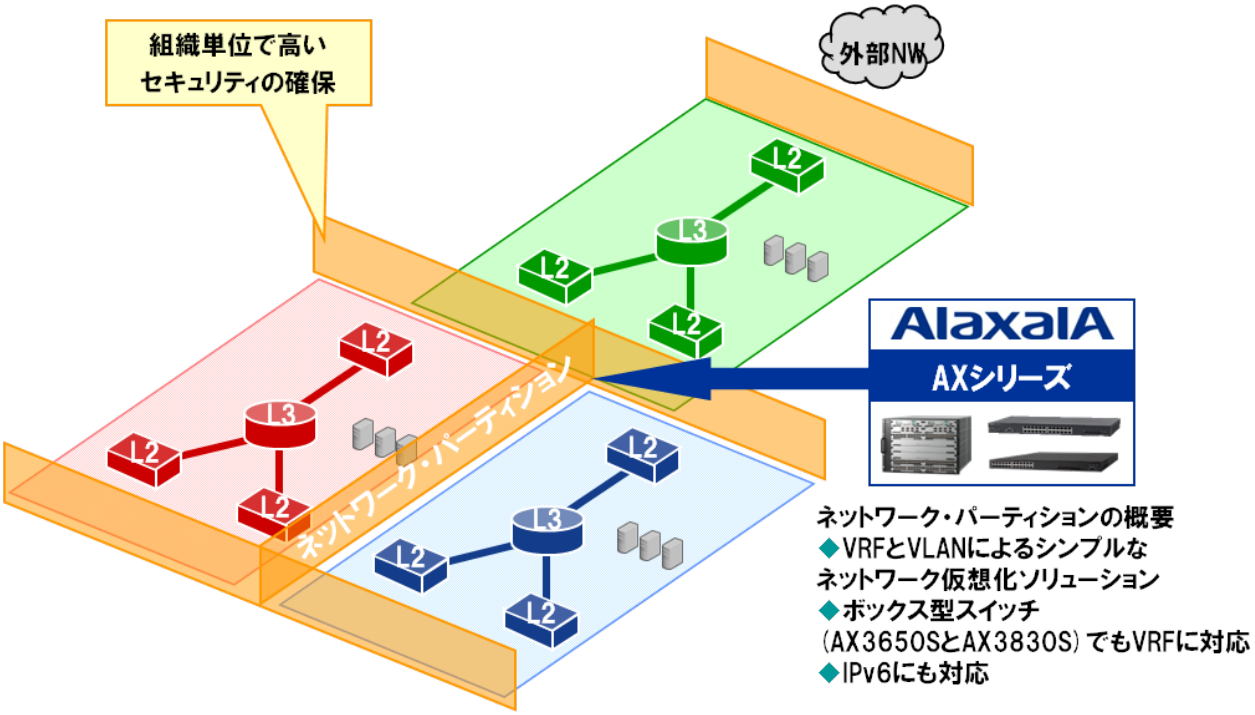


図 1.3-1 ネットワーク・パーティションによる仮想ネットワーク概念図

ネットワークごと組織単位に分離するため、組織間の通信を完全に遮断することができます。
しかし、ネットワーク自体はネットワーク・パーティションによる仮想ネットワークで構成されるため、実際のスイッチ機器は最少の構成で済み、機器や運用コストの増加を抑えます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

1.3.2 ファイアウォールの仮想化

ネットワーク・パーティションによって組織毎に分けられたネットワークそれぞれに対する、外部からの脅威の防御や内部からのアクセス制御、管理、監視については、やはりそれぞれのネットワークにファイアウォールを配置するのがシンプルでわかりやすい構成でしょう。

そのネットワークそれぞれに渡るいくつものファイアウォールを、パロアルトネットワークスPAシリーズによる仮想ファイアウォール機能、仮想システム(VSYS)が担います。

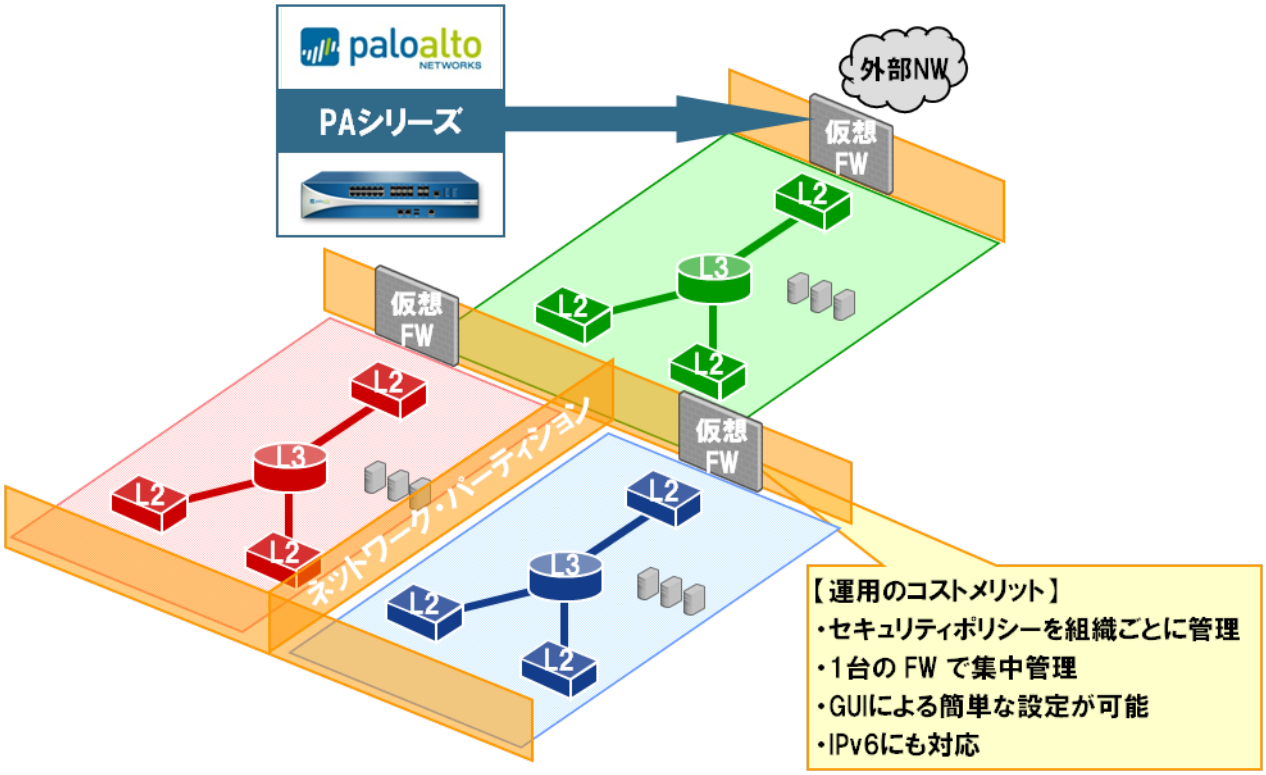


図 1.3-2 仮想ファイアウォール適用の概念図

ネットワーク・パーティションによる仮想ネットワークで構成された組織毎のネットワークそれぞれに対し、仮想ファイアウォール(VSYS)をそれぞれ配置することで、組織毎のアクセス管理や監視を、同じく最小限の投資で済ませることが可能です。

またVSYSは単なるファイアウォールとしてだけではなく、パロアルトネットワークスPAシリーズならではの「アプリケーション」、「ユーザ」、「コンテンツ」の3つの要素に対する全レイヤでセキュリティを提供する仮想ファイアウォールとして機能します。このためアプリケーションごとの細かな設定や使用者の識別も可能な柔軟かつ堅牢なセキュリティを、組織毎に提供しその組織自体を守るだけでなく、万が一の組織内部からの攻撃やウイルス感染の脅威をその組織内など局所的に留め、他の組織への影響を防ぐ、といった高度なセキュリティを実現します。

このように、アラクサラのネットワーク・パーティションと、パロアルトネットワークスPAシリーズのVSYSの組み合わせにより、組織毎に独立して高度で強固なセキュリティ管理とユーザレベルに合わせて自由度が高く使いやすいネットワークを最小限の装置機器構成で構築することができます。

システム全体として高度なセキュリティ環境を実現しながらも、機器の構成と運用管理コストについては最小化の両立を図ったシステムを作ることを可能にする。それが「セキュア仮想ネットワークソリューション」です。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

2. キーテクノロジ

ここでは、先に述べた「2 つの仮想化」それぞれについて、より詳細に解説します。

2.1 ネットワーク・パーティション（VRF機能）

アラクサラが提供する、ネットワークにおける仮想化技術がネットワーク・パーティションです。

ネットワーク・パーティションとは、レイヤ 3 機能を論理的に分割する『VRF(Virtual/VPN Routing and Forwarding)』と呼ばれる機能に、レイヤ 2 の論理ネットワーク技術である VLAN を組合せ、複数の論理的なネットワークをシンプルな物理構成によるシステムで実現する技術です。

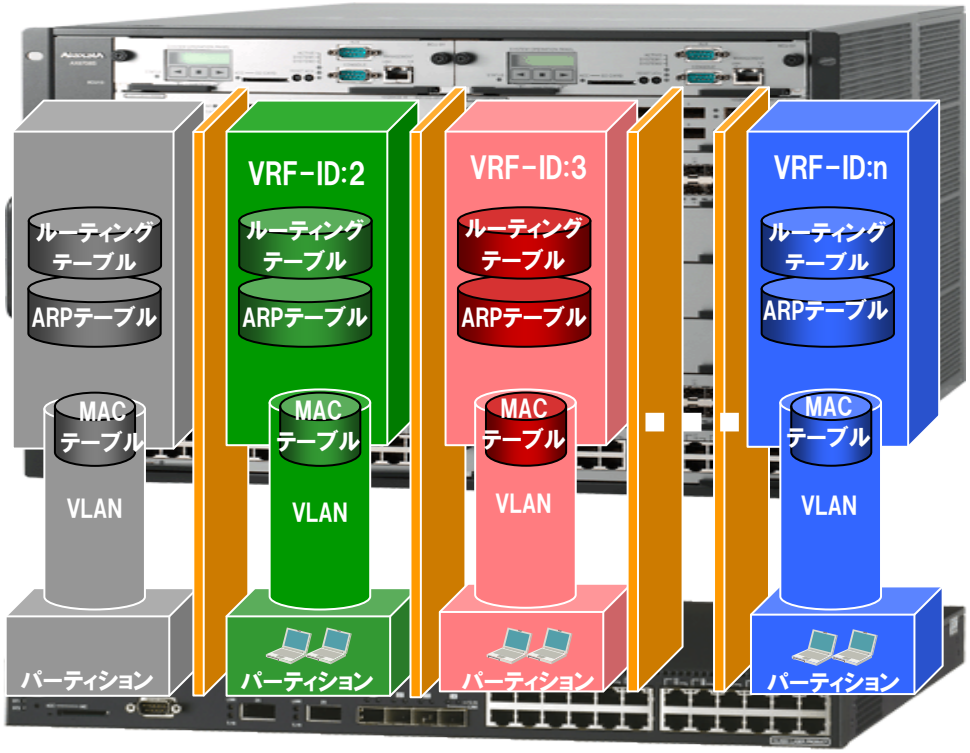


図 2.1-1 ネットワーク・パーティション概念図

VRF では、レイヤ 3 ネットワークでの基本情報であるルーティングテーブルや ARP テーブルなどを、扱う複数のネットワークそれぞれで独立して制御および管理をおこないます。この VRF によって分けられた論理的なレイヤ 3 ネットワークと VLAN によって分けられた論理的なレイヤ 2 ネットワークを、分割されたネットワーク単位でまとめたものを「パーティション」と呼びます。

これにより、レイヤ 3 のネットワークが論理的にいくつもあるようなシステムを 1 台で構成することが可能となるため、組織単位で独立したネットワーク構成とすることも簡単にできます。

ただし、VLAN およびルーティングテーブルや ARP テーブルは、装置の持つ全体のリソースを各 VRF で分けあって使用します。従って VRF によって装置の収容条件等が拡張されるものではありません。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

VRF を扱う装置内では、VRF-ID と呼ぶ VRF 毎にユニークな識別子を各パーティション内の VRF や VLAN に付与して区別しますが、システム全体の管理用などに VRF-ID を持たないパーティションによるネットワークも存在します。これをグローバルネットワークと呼び、グローバルネットワークでは telnet や FTP、syslog などシステム管理に関する機能が一般の VRF より広くサポートされます。

AX シリーズにおいて VRF 機能をサポートする機種および設定可能な VRF 数は以下の通りです。

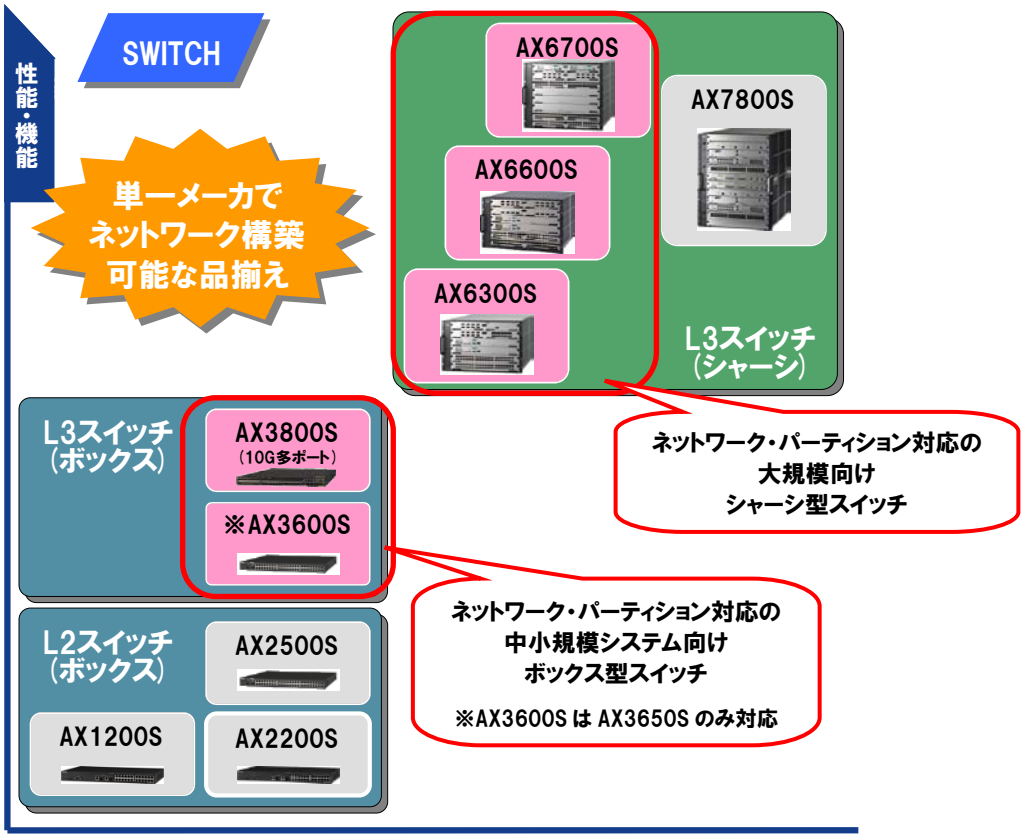


図 2.1-2 ネットワーク・パーティション対応の AX シリーズ

表 2-1 VRFサポート状況

VRF サポート機種	シャーシ型			ボックス型	
	AX6700S	AX6600S	AX6300S	AX3830S	AX3650S
VRF 設定可能数 （グローバル含まず）	63/124/249 (*1)	63/124/249 (*1)	63/124/249 (*1)	31	31

(*1)同時に使用する L2 冗長プロトコルの有無や種類によります。

ネットワーク・パーティションのさらに詳しい内容については、「AX シリーズ ネットワークパーティション ソリューションガイド [基本編] [認証編] [応用編]」に記載しています。こちらも合わせてご利用ください。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

2.2 パロアルトネットワークスPAシリーズと仮想ファイアウォール(VSYS)

今回のソリューションで用いるパロアルトネットワークスの PA シリーズは、「次世代ファイアウォール」として位置づけられるもので「アプリケーション」、「ユーザ」、「コンテンツ」の各要素に対して、全レイヤでセキュリティを提供できることが最大の特長となっています。

このため誰がどのアプリケーションを使用しているかの識別ができ、ユーザやアプリケーションごとに「書き込みは NG」、「閲覧は OK」といった細かな設定も可能となっています。また対応できるアプリケーションも 1300 種類を超え、これらを「アプリの見える化」により柔軟かつ堅牢なセキュリティを実現します。

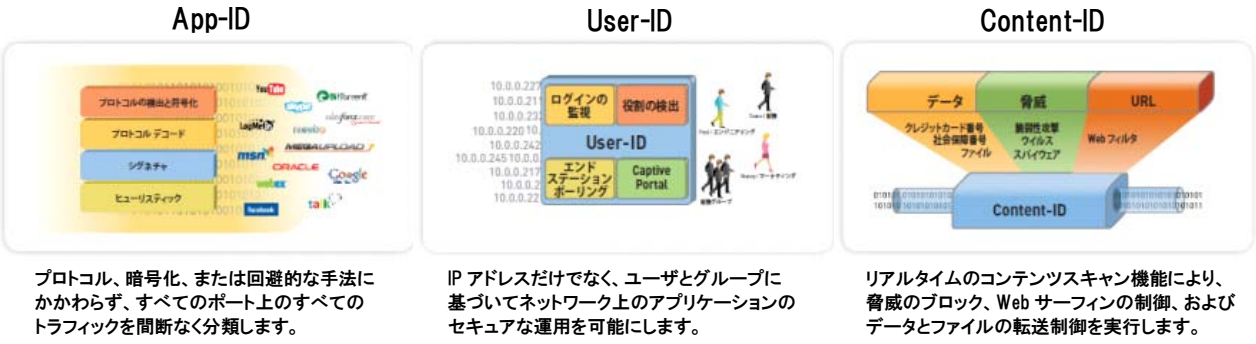


図 2.2-1 パロアルトネットワークス PA シリーズのコアテクノロジ

また一般の UTM 装置では、すべての機能をフルに使った場合にパフォーマンスが著しく低下するものもありますが、パロアルトネットワークス PA シリーズでは専用設計のハードウェアとそれに密接にインテグレーションされたソフトウェアエンジンにより、フルに機能を使ってもパフォーマンスが著しく低下することはありません。

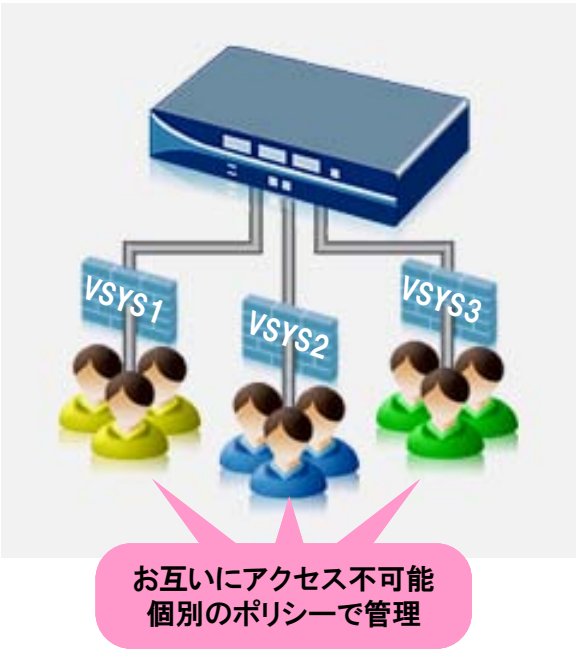


図 2.2-2 VSYS のイメージ

そしてパロアルトネットワークス PA シリーズの上位機種(PA-2000 シリーズ以上)では、仮想システム(VSYS)という仮想ファイアウォールの機能を備えます。

VSYS とは、物理的な1台のパロアルトネットワークス PA シリーズにおいて、あたかも複数のファイアウォールがあるかのようにふるまう機能であり、装置内では個別に管理され独立した仮想的なファイアウォールとして扱われます。そのため、VSYS によって分けられている他のユーザからは、自らの VSYS に対しアクセスされたり閲覧されたりすることなく、また各 VSYS でそれぞれ個別のポリシーを持って運用することも可能です。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

ネットワークに VSYS を加える場合、各 VSYS は以下の動作モードで構成することができます。これらのモードについても各 VSYS 毎に独立して設定が可能です。

- VirtualWire モード
  2 つのポート間でスイッチングやルーティングをおこなわない真のトランスペアレントなモード。
- Layer2 モード
  同一ネットワークセグメント(VLAN)内でファイアウォールとして機能するモード。
- Layer3 モード
  異なるネットワークセグメント(VLAN)にまたがりゲートウェイ的に動作するモード。
  NAT などを使う場合はこのモードで使用することが前提となります。

このように VSYS を用いると、複数のネットワークシステムにおいてパロアルトネットワークス PA シリーズの持つ次世代ファイアウォールの優れた機能をそれぞれで活かしながらも実際には最小限の装置数で済ませることができるため、システム全体として高いコストパフォーマンスと運用性を実現することができます。

また、パロアルトネットワークス PA シリーズはラインアップも豊富であり、様々なシステム規模に対応します。

図 2.2-3 パロアルトネットワークス PA シリーズ

表 2-2 VSYSをサポートする機種とVSYS数

VSYS 対応機種	PA-2020	PA-2050	PA-5020	PA-5050	PA-5060
FW スループット	500Mbps	1Gbps	5Gbps	10Gbps	20Gbps
VSYS 数	1 (※最大 6)		10 (※最大 20)	25 (※最大 125)	25 (※最大 225)

※VSYS アップグレードライセンスの購入が必要です。

VSYS は PA-2000 シリーズや PA-5000 シリーズでサポートされ、アップグレードライセンスを追加することで VSYS 数を拡張することができます。性能も PA-5050 では 10Gbps、PA-5060 においては 20Gbps のファイアウォールスループットインタフェースを備えるなど、大規模なネットワークシステムにも対応できます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

2.3 仮想化テクノロジーの組み合わせによるメリット

以上、アラクサラのネットワーク・パーティションと、パロアルトネットワークス PA シリーズの仮想システム(VSYS)を組み合わせることで、次のようなメリットが得られます。

➢ミニマムな物理的制約

物理構成(装置台数)の最小化により、導入コストや電力/スペースなどを低減。また管理対象も少なくなり、運用コストも低減。

➢自在な論理構成

論理構成は自在なので物理構成はシンプルなまま、高度なネットワークを構成することが可能。

➢システム変更への柔軟な対応

仮想ネットワークは他の仮想ネットワークにほぼ影響無く追加削除や変更が自由。組織の統合や部署の新設などに対して柔軟な対応が可能。

➢IPv6 Ready

AX シリーズ、パロアルトネットワークス PA シリーズとも IPv6 に対応。IPv6 マイグレーションにも対応が可能。

➢ネットワーク認証とも連携

AX シリーズのネットワーク認証機能と連携することで、ロケーションに縛られずに自分のリソース(仮想システム)へアクセスすることが可能。

これらより設備投資や運用コストの軽減、拡張性を高め事業効率の向上などが期待でき、実システムへの適用も例えば大規模エンタープライズ環境へのマネージドサービスの提供手段として、以下のような用途が考えられます。

- データセンタにおける、顧客別の独立したネットワークセキュリティサービス
- 事務、教員、学生などセキュリティレベルの異なるネットワークそれぞれに対する、独立したネットワークセキュリティゲートウェイの提供
- 社内での Twitter, Facebook など各種 SNS や特定アプリケーションの利用制限
- プライベートクラウドサービスでの独立したネットワークセキュリティゲートウェイオプションサービス
- 同じプライベートアドレスを持つネットワーク同士のアドレスの変更を伴わない統合

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

2.4 セキュア仮想ネットワークの具体化イメージ

以上、2 つの仮想化技術によって提唱されるセキュア仮想ネットワークソリューションを、実際のシステムとして適用し構築するとどのようになるのか、どのようなメリットがあるのかについて解説します。

まず、会社などで使われるネットワークは、一般的には図 2.4-1 のようなイメージで考えられます。

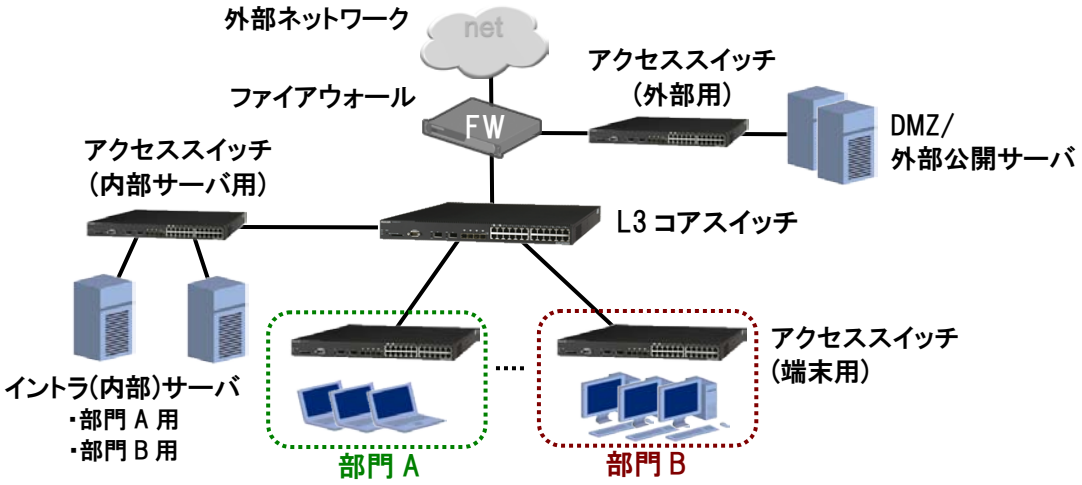


図 2.4-1 一般的なネットワーク構成

このようなネットワークシステムを、セキュア仮想ネットワークで構成すると、

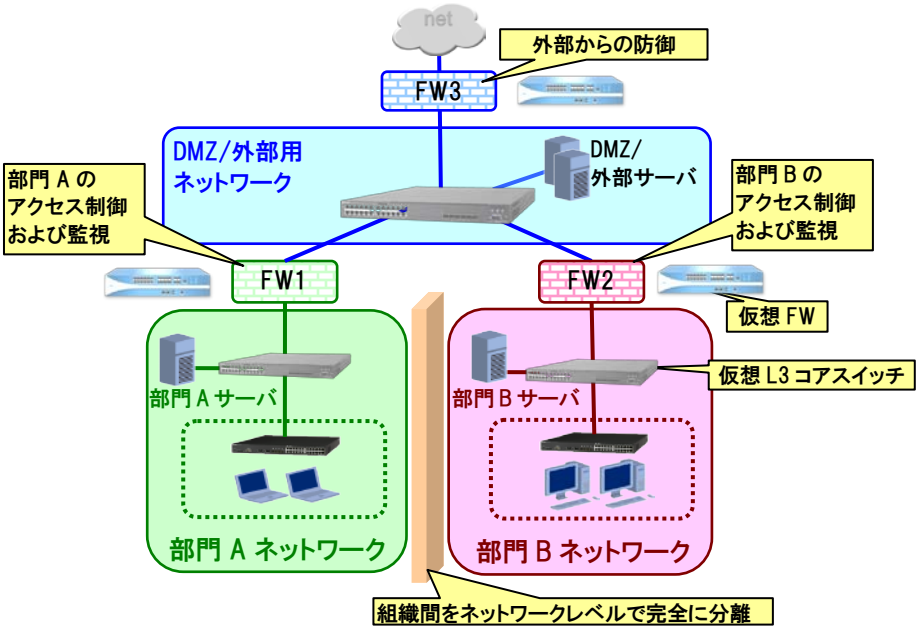
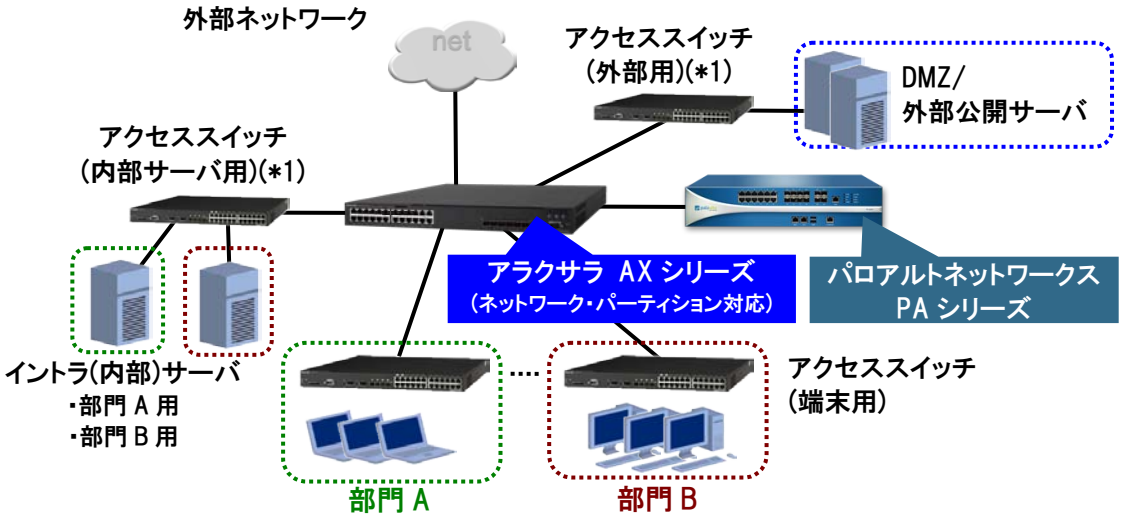


図 2.4-2 セキュア仮想ネットワークの論理構成

図 2.4-2 のように、組織ごとにネットワークとアクセス制御が分離された、高度なセキュリティを備えるネットワークとすることができます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

しかしながら、このネットワークを実現する装置の構成は図 2.4-3 の通りとなり、初めに提示した図 2.4-1 の単一ネットワーク構成とほとんど変わらない構成となります。このように仮想化技術によって、最小限の装置機器およびその管理で、組織ごとに分けられたネットワークを運用できることがわかります。



(*1)実際は VLAN でわけられているため、サーバ用スイッチは外部用/内部用でまとめても良い。

図 2.4-3 セキュア仮想ネットワークの物理構成

2.5 装置の冗長化

さらに、実際に運用されるシステムでは、装置機器や回線の障害などに対応できるよう可用性を考慮した構成とするケースが一般的ですが、複数のネットワークが同一の装置上に構成される仮想ネットワークでは、より高い信頼性が要求されるため、システムとして冗長構成は必須です。

アラクサラの AX シリーズでは、FT スイッチ（AX6700S/AX6600S/AX6300S）や、スタック機能、リング、GSRP 等に代表される高信頼、高可用を実現する機能の他、STP/VRRP 等の標準化された装置冗長プロトコルも利用可能です。これら各機能の詳細やシステム構築の方法等については、構成に応じて当社 Web ページ等にて各種構築ガイドを揃えていますのでご活用ください。

一方、パロアルトネットワークス PA シリーズにおいても、HA（High Availability：冗長化構成）機能により、冗長構成のシステムを構築することができます。アクティブ/パッシブまたはアクティブ/アクティブ高可用性のいずれかがサポートされ、セッションおよび設定の同期化機能も完備されています。HA 機能では、まったく同じに設定された 2 台の装置間でハートビート コネクションが張られているため、装置に障害が発生した場合でもシームレスなフェイルオーバーが確実に実行されます。

(i) アクティブ/パッシブモード動作概要

- アクティブ装置は HA インターフェイスを介し設定情報とセッション情報をパッシブ装置と継続的に同期します。
- アクティブ装置で障害が発生すると、パッシブ装置がハートビートの喪失を検出して自動的にアクティベーションされます。
- 1 つの HA インターフェイスに障害が発生しても、残りのインターフェイスで同期を続行するよう設定が可能です。なお状態同期用の接続 (HA2 リンク)が失われると、状態が同期されなくなります。設定同期用の接続 (HA1 リンク)が失われると、設定が同期されなくなり、さらに HA 装置間のハートビートも喪失します。このとき両方の装置ではもう一方の装置がダウンしていると判断され、両方の装置ともアクティブになります。
- 管理ポートは、ハートビートバックアップ設定オプションを使用して、ハートビートおよび hello メッセージのバックアップパスとなるように設定できます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(ii) アクティブ/アクティブモード動作概要

アクティブ/アクティブモードでは以下の 3 つの動作を選択できます。

- **Static interface IP**
  HA を構成する互いの装置で異なる静的 IP アドレスを持ち、動的ルーティングのイコールコストマルチパス等を用いてレイヤ 3 的にトラフィックを分散して扱えるようにするモードです。
- **Floating IP**
  このモードは、HA を構成する装置の状態に関係なく 共通の IP アドレスを使用可能にする必要がある場合など、VRRP (Virtual Router Redundancy Protocol)のような機能が必要な場合に使用します。各装置では共通な IP アドレスを所有できるように、特定のインターフェイスに 2 つのフローティング IP アドレスを設定します。
- **ARP load sharing**
  このモードは、ARP (Address Resolution Protocol) を使用して 2 つの装置間でホストトラフィックの負荷を分散するときに使用します

以下、2.4節で紹介したセキュア仮想ネットワークの物理構成を冗長構成とした例を以下に示します。論理的な構成は「図 2.4-2 セキュア仮想ネットワークの論理構成」と変わりません。

(1) FTスイッチ＋パロアルトネットワークスPAシリーズHA構成

比較的大規模なシステムで、L3 コアのスイッチが AX6000S ファミリ等のシャーシ型となる場合、FT 構成として、シンプルに高信頼なシステムを構成することができます。

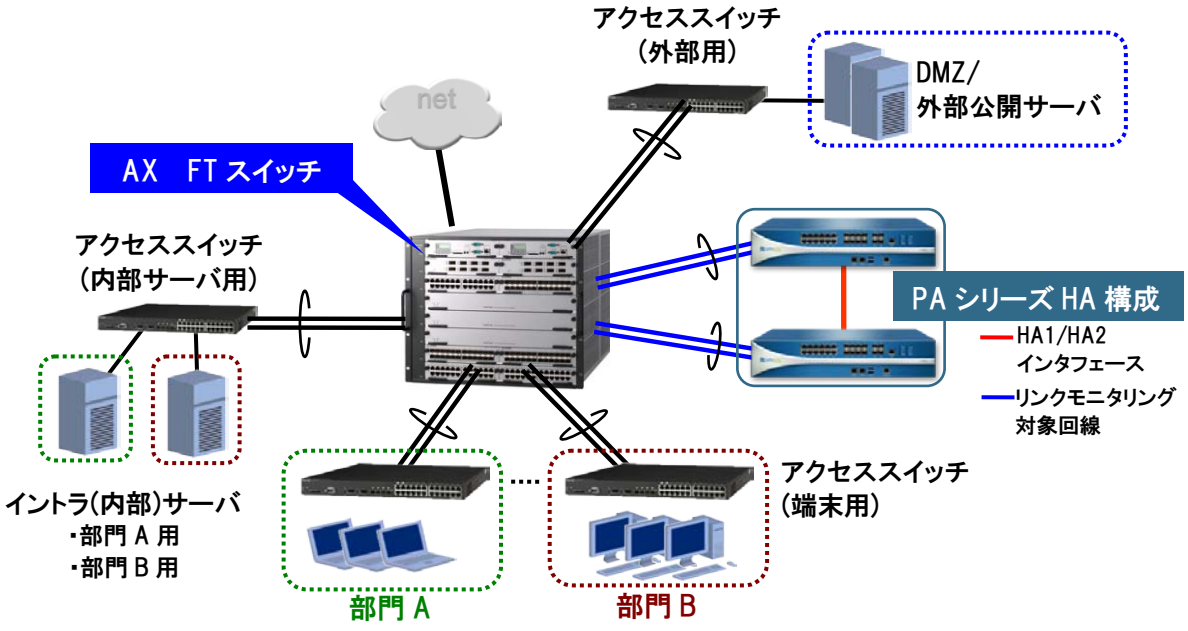


図 2.5-1 FT スイッチ＋PA シリーズ HA 構成

FT スイッチと周辺スイッチの接続はリンクアグリゲーションでの接続が基本ですが、パロアルトネットワークス PA シリーズとの接続においては、スタティックモードのリンクアグリゲーションによる接続となります。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(2) スタック構成 ＋パロアルトネットワークスPAシリーズHA構成

中小規模のシステムで、L3 コアスイッチを AX3650S 等のボックス型で構成するといった場合は、スタック機能によるスタック構成と組み合わせ、以下のような構成とすることができます。

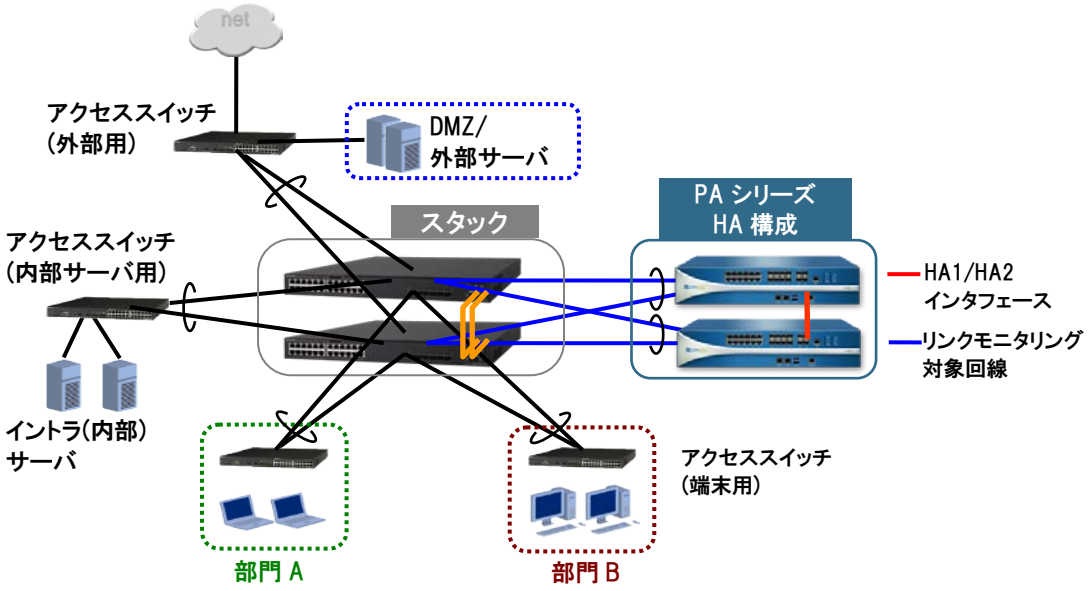


図 2.5-2 スタック構成 + PA シリーズ HA 構成

この構成においても、パロアルトネットワークス PA シリーズとの接続はスタティックリンクアグリゲーションを基本として接続することを推奨します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3. システム構築例

これまでの解説の通り、アラクサラのネットワーク・パーティションによる仮想ネットワークとパロアルトネットワークスPA シリーズ(以下 PA シリーズ)の仮想システム(以下 VSYS)による仮想ファイアウォールを使うと、最小限の装置機器の運用で複数のネットワークとアクセス制御による高度なセキュリティを持つネットワークを構成できます。

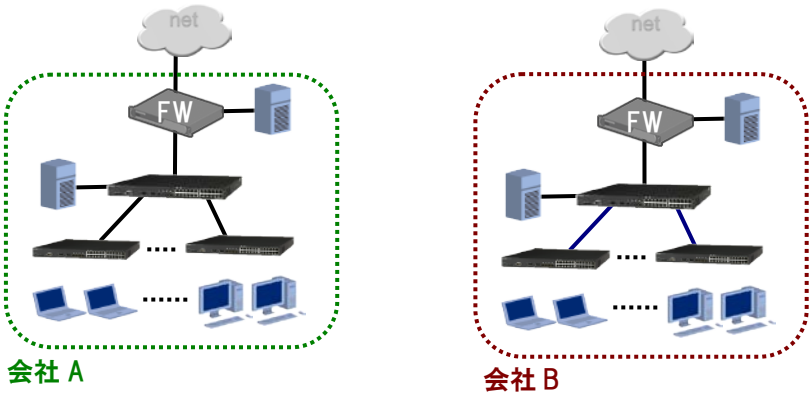
本章では、2.4 節で紹介した構成をもとに、

- FT スイッチと PA シリーズ HA 構成での構成例
- スタック構成としたボックス型スイッチと PA シリーズ HA 構成での構成例

それぞれを構築する場合について解説します。

3.1 完全システム分離構成の適用例（FTスイッチ+PAシリーズHA構成）

仮想ネットワークは全く独立した複数のシステムを収容できます。以下に、既に稼動中の複数ネットワークを仮想ネットワークとして収容する場合の構築例について示します。物理的には一つのシステムであっても、仮想ネットワークにてまったく独立分離したネットワークとして扱うため、端末やサーバの設定はこれまでのネットワークと設定を変更することなく利用することが可能です。



用途	VLAN ID	IP アドレス
会社 A 外部接続用	1000	10.10.1.0/24（外部）
会社 A サーバ用	10	10.0.0.0/16
会社 A PC 用	100-101	192.168.0-1.0/24
会社 B 外部接続用	1000	10.20.2.0/24（外部）
会社 B サーバ用	20	20.0.0.0/16
会社 B 端末 PC 用	100-101	192.168.0-1.0/24

図 3.1-1 2 つの独立したネットワーク

ここでは、以上のように 2 つの会社の全く独立したネットワークを例に考えます。この会社 A と会社 B のネットワークを一つのネットワークシステムに再構築することを考えた場合、相互の会社ネットワーク間を確実に分離するフィルタの設定が必須であったり、会社毎に異なるセキュリティポリシーに基づいた設定がファイアウォールにそれぞれ必要であったり、またもともとが互いに独立したネットワークであるため使用している IP アドレスが重複することがあるなど、そのまま一つのシステムに統合するのは困難かと思われます。

このようなケースにおいて、セキュア仮想ネットワークソリューションが最適です。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

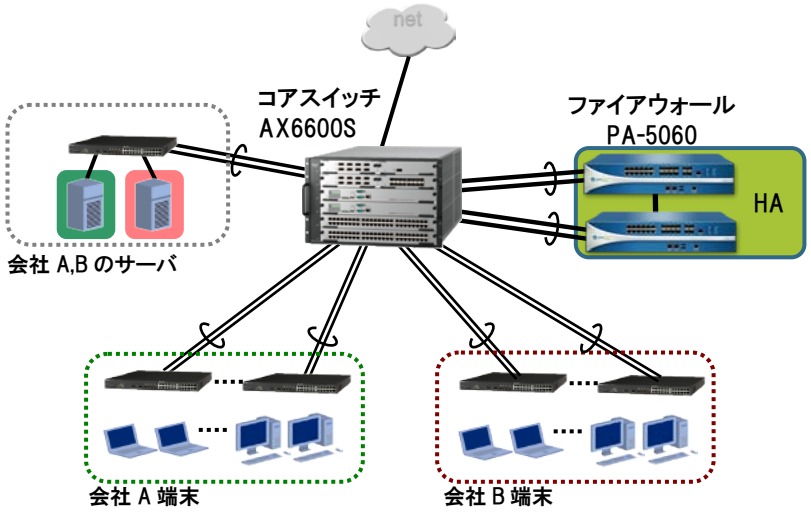


図 3.1-2 仮想ネットワークによる会社 A,B 統合システムの物理構成

セキュア仮想ネットワークソリューションでは、物理構成は以上のように単一のネットワークとほとんど変わらない構成となります。ネットワークは FT スイッチによる構成で高い可用性を確保し、ファイアウォールについては、PA シリーズをアクティブ/パッシブの HA 構成で使用してネットワークのコア部分に組み込みます。

そして、ネットワークパーティションによる仮想ネットワークと VSYS による仮想ファイアウォールで構成される論理構成は以下の通りとなり、会社 A、会社 B それぞれのネットワークを完全に独立分離して収容する形となります。

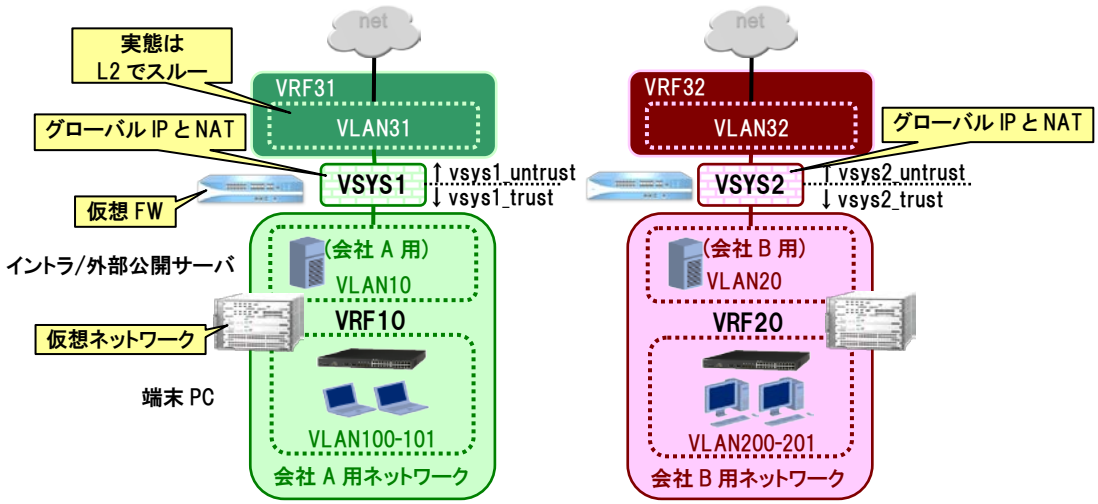


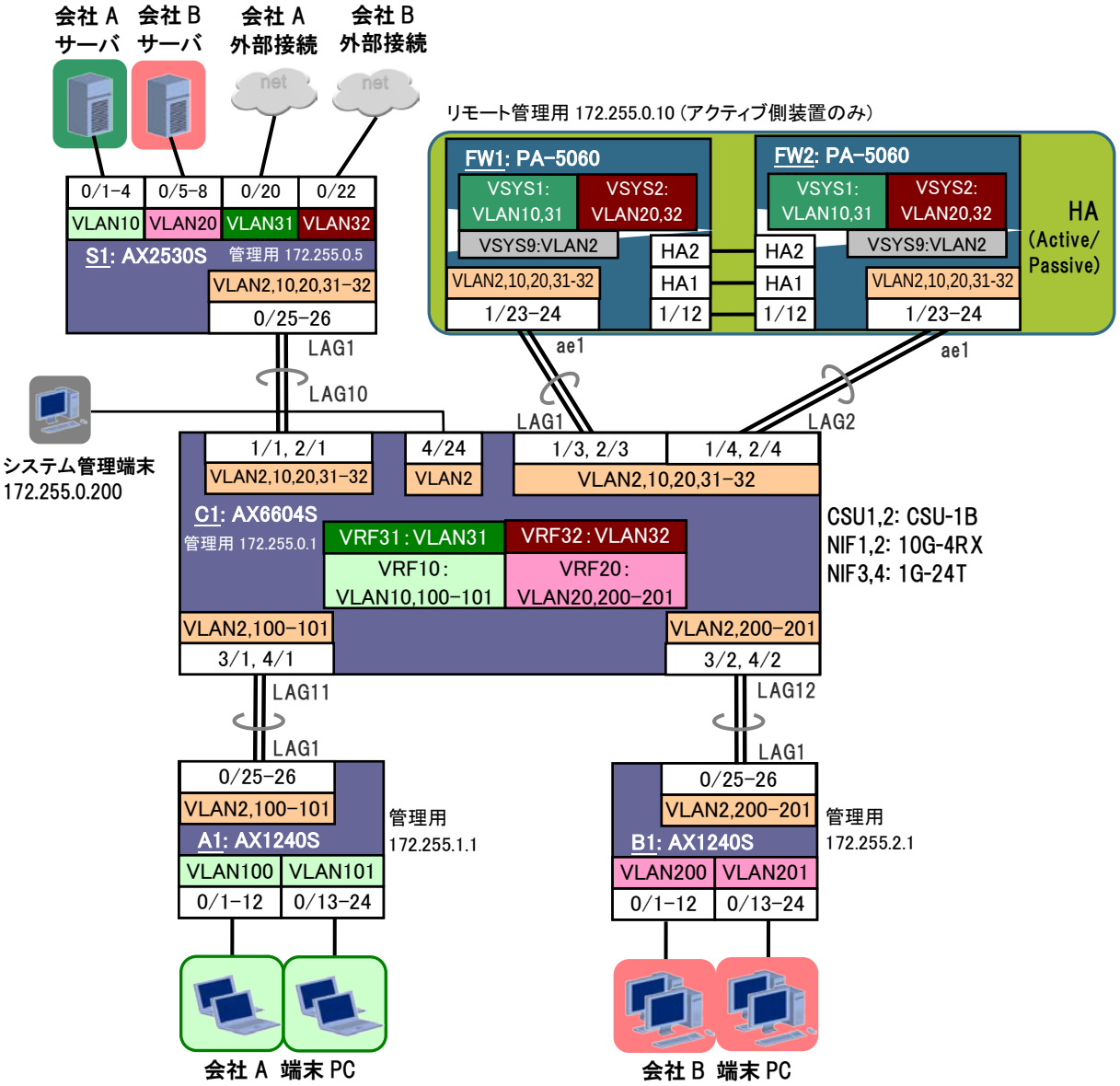
図 3.1-3 会社 A,B システムの論理構成

具体的には、ネットワーク・パーティション(VRF)による仮想ネットワークにて会社 A、会社 B の内部ネットワークそれぞれを収容し、また外部ネットワークとのファイアウォールについても、VSYS による仮想ファイアウォールにてそれぞれのネットワークの外部接続用ファイアウォールとして機能するように構成します。

これにより、会社 A,会社 B から見ると今まで同様なネットワーク環境が、物理的な一つのネットワークに収容することができます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

このネットワークにおける、各装置ごとでの論理構成は以下のようになります。



用途	VSYS	VRF ID	VLAN ID	IP アドレス（*1）
会社 A 外部接続用	VSYS1	31	31	31.0.0.0/24（外部ルータ: .254）
会社 A サーバ/Uplink 用		10	10	10.0.0.0/24
会社 A 端末 PC 用	–		100-101	192.168.0-1.0/24
会社 B 外部接続用	VSYS2	32	32	32.0.0.0/24（外部ルータ: .254）
会社 B サーバ/Uplink 用		20	20	20.0.0.0/24
会社 B 端末 PC 用	–		200-201	192.168.0-1.0/24
システム総合管理用	VSYS9	global	2	172.255.0.0/16

（*1）ホストアドレス x.x.x.1 は装置 C1 で、x.x.x.10 は装置 FW1/FW2 で使うものとする。

図 3.1-4 会社 A,B 統合システム 論理設定詳細

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.1.1 システム構築時のポイント

本例の構成を設計する際におけるポイントを以下に示します。

(1) コアスイッチ、ファイアウォールの要求性能や収容条件は元システムを集約した分が必要。

複数のネットワークをそれぞれ仮想ネットワークとして扱い物理的にはひとつの構成に集約する場合、もとのネットワークで必要な性能や収容条件の和を超える性能や収容能力が必要となります。

従って使用する装置の選定に関しては、もとのネットワークそれぞれで使用していた装置の必要性能や収容条件の総和を目安とすれば良いでしょう。

(2) 可用性の確保はフォールト・トレラント(FT)構成で。ファイアウォールはHA構成で。

本例のようにコアに AX6700S/AX6600S/AX6300S といったシャーシ型のスイッチを用いる場合では、装置の可用性確保にはフォールト・トレラント構成(装置内モジュールを冗長とした構成)を推奨します。またファイアウォールであるパロアルトネットワークス PA シリーズについては 2 台の装置で HA 構成とします。

(3) コアスイッチとファイアウォール間はリンクアグリゲーションで接続する。

コアスイッチとファイアウォール装置間の接続については、リンクアグリゲーション(PA シリーズでは Aggregate Ethernet インタフェースと呼びます)を用いて回線の可用性を確保します。

(4) 各仮想ネットワークと外部ネットワーク間のファイアウォールは仮想ファイアウォールにてそれぞれ構成する。

既存のネットワークを収容する場合、もとのネットワークで持っていたグローバル IP アドレスをそのまま引き継ぐケースが多いと思われます。

従ってそれぞれのネットワークでの外部への接続はそれぞれのネットワークに割り当てる VSYS を用いて直接外部と接続するように設定します。VSYS ではネットワークアドレス重複の許容はもちろん、NAT も VSYS ごとに独立して機能します。

(5) PAシリーズはインターネットと接続できるパスを設ける。

PA シリーズのライセンス管理や各種フィルタ機能で使用されるパターンファイル、シグネチャ等の更新などは外部にある専用サーバを通しておこないます。従って PA シリーズはインターネット接続できる環境下に置く必要があります。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.1.2 スイッチ(AXシリーズ)設定時のポイント

コンフィグなど、機器の設定の際のポイントを以下に示します。

(1) シャーシ型スイッチ(AX6700S/AX6600S/AX6300S)でVRFを使用する場合、モードを設定する。 AX Serise

シャーシ型のモデル(AX6700S/AX6600S/AX6300S)でネットワーク・パーティション(VRF)を使用する場合、VRF の動作モードを設定する必要があります。また本設定の際にはスイッチング機構(BSU、CSU、MSU)が再起動されます。

(2) VLANインタフェースでの設定は最初に所属VRFの設定からおこなう。 AX Serise

VLAN インタフェースでは、所属 VRF の設定と IP アドレスの設定が必要ですが、所属 VRF の設定は IP アドレスの設定前におこなう必要があります。(IP アドレスが設定されている状態では所属 VRF の設定はできません。)
ですので、VLAN インタフェースの設定では所属 VRF の設定を最初におこなってください。

(3) PAシリーズと接続するポートについてはスタティックのリンクアグリゲーションとする。 AX Serise

PA シリーズとの接続は Aggregate Ethernet インタフェースを通じておこないます。これはいわゆるスタティックのリンクアグリゲーションと同等の機能のため、AX スイッチ側ではスタティックのリンクアグリゲーションを構成して接続します。

3.1.3 ファイアウォール(パロアルトネットワークスPAシリーズ)設定時のポイント

同様に、PA シリーズの設定におけるポイントを以下に示します。

(1) コンフィグ他、各種機能等の設定作業はアクティブ装置のみに対しておこなえば良い。 PA Serise

以下(4)でも述べますが、HA を構成する装置間の設定内容は同期させることが可能です。従って HA を構成するシステムでは各種設定の変更作業および commit はアクティブ側の装置に対してのみおこなえば良いです。

(2) HA構成とする場合、最低限HA1 は冗長接続を推奨。 PA Serise

PA シリーズにて HA 構成を組む場合、2 台の装置間にて Control-Link(HA1)および Data-Link(HA2)(アクティブ-アクティブ構成の場合 HA3 も)というインタフェースの接続が必要です。可能であれば HA1,HA2,HA3 各リンクとも冗長接続とすることが最も望ましいですが、空きポートに余裕が無い場合など、HA 用ポートが十分に用意できない場合は最低限 HA1 だけでも冗長に接続することを推奨します。
Contorl-Link である HA1 は装置間で優先度を決める(アクティブ-パッシブ構成の場合アクティブ側を決める)情報をやりとりしており、HA1 がリンクダウンするといわゆるダブルアクト状態に陥ります。

なお HA1、HA2 については上位機種(PA-4000 シリーズ、PA-5000 シリーズ)の場合、専用のポートがありますが、一般の Ethernet ポートも HA インタフェースとして HA1～HA3 用に割り当てることができるため、HA 用に冗長接続をおこなう場合は一般の Ethernet インタフェースを HA インタフェースに適宜割り当てて冗長経路を追加します。

(3) HAでアクティブとする予定の装置は、プライオリティ設定値をデフォルトより小さい値とする。 PA Serise

2 台以上の装置でアクティブ/パッシブ高可用性(HA)構成とする場合、アクティブ/パッシブとなる装置の優先付けとしてプライオリティを設定します。プライオリティは設定値の小さい方が優先されます。

アクティブ/パッシブでの HA 構成をイネーブルとした装置間で Control-Link(HA1)が確立すると、プライオリティ設定値の小さい側の装置がアクティブとなります。このため、アクティブとしたい装置のプライオリティはデフォルトの値(=100)より小さく設定することを推奨します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(4) HA構成を確認したらコンフィグを同期させること。 PA Serise

HA を構成する場合、ネットワークの論理的に矛盾のないようコンフィグ等の設定も HA 構成の装置間で一致させておく必要がありますが、PA シリーズでは HA 構成の装置間にてコンフィグを同期させる機能があります。
ただしそのコンフィグ同期は自動的にはおこなわれませんので、コンフィグを同期させる際はアクティブ側装置(コンフィグ同期元装置)での GUI 上のコンフィグ同期指示(Dashboard タブ-High-Aveilability ウィジェット中の「sync to peer」 

をクリック)もしくは CLI での同期コマンド実行、あるいは commit 実行をおこなってください。

(5) AXと接続するポート(物理インタフェース)はAggregate Ethernetインタフェースとする。 PA Serise

PA シリーズの上位機種では、回線インタフェースに Aggregate Ethernet インタフェースと呼ぶスタティックリンクアグリゲーション相当の機能があります。AX シリーズスイッチへの接続は、この Aggregate Ethernet インタフェースによりおこなう設定とします。

(6) ネットワーク設定ではゾーンや所属VSYS、仮想ルータ等の設定も忘れずに。 PA Serise

PA シリーズでのネットワークに関する設定では、Ethernet インタフェースや、VLAN を使用する場合の VLAN の設定などの他に、ファイアウォールのポリシー設定等で使用するゾーンの設定が必要です。さらに VSYS を使う場合は所属する VSYS、また Layer3 のインタフェースでは対応させる仮想ルータの設定などが必要となります。これらが設定されていない場合、正しく通信をおこなうことができません。

なお、GUI におけるゾーンや VSYS、仮想ルータ等の設定は Ethernet インタフェースや VLAN の設定画面からも設定のウインドウを呼び出せるようになっています。

(7) PAシリーズはデフォルトではpingに応答しないため注意。 PA Serise

システム構築の際、ネットワークの到達性確認のため ping を使って疎通確認をおこないたいケースもあるかと思いますが、PA シリーズの Layer3 インタフェース(IP アドレスを持つ Ethernet ポートや VLAN)を ping の宛先とした場合、ネットワークに到達性があってもそのままでは ping に応答しません。
PA シリーズのインタフェースにて ping 応答をさせたい場合は、ping 応答を許可する Layer3 インタフェースに対し、あらかじめ Management Profile にて ping を許可する設定としたプロファイルを適用する必要があります。

同様に、管理ポート以外で telnet や Web-GUI(http/https)による装置の管理をおこなう場合も、同様に Management Profile にて管理用のプロファイルを用意し、インタフェースに適用する必要があります。

(8) 必要に応じて各ネットワーク毎の管理ユーザを設定する。 PA Serise

デフォルトで用意されている管理ユーザ(admin)では、各 VSYS の設定はもちろん、ライセンス管理やシグネチャのアップデートなど、PA シリーズ装置全体の管理をおこなうことができますが、新規に管理ユーザを設定する際には、単一または特定の VSYS など、管理できる範囲を設定することができます。
ですので、管理単位の独立した仮想ネットワークにて VSYS を使用する際には、各ネットワークで独立した管理者を割り当てられるよう、各ネットワーク(各 VSYS)向けの管理ユーザを設定することを推奨します。

(9) 設定の最後には必ず「Commit」をおこなうこと。 PA Serise

PA シリーズの設定では、各設定で[OK]を選択して設定を終了しても、実行中のコンフィグ(Running Configuration)へはリアルタイムには反映されません。GUI による設定でも CLI による設定でも最終的に入力した設定を装置に反映させる(Candidate Configuration を Running Configuration へ反映させる))ためには Commit コマンドの実行が必要です。
また、HA を構成している場合、アクティブ装置での Commit 実行が正しくおこなわれると、そのままパッシブ装置へのコンフィグ同期もおこなわれます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.1.4 コンフィグレーション例

本構成のコンフィグレーションの例を下記に示します。

(1) コアスイッチ (AX6600S)の設定

C1 (AX6604S) の設定

スパニングツリーの抑止

```
(config)# spanning-tree disable
```

AX シリーズではデフォルトで PVST+が有効になっており、FT 構成とする場合にはこれを抑止します。

VRF の設定

```
(config)# vrf mode l2protocol-disable
All CSU will be restarted automatically when the
selected mode differs from current mode.
Do you wish to change mode (y/n): y
(config)# vrf definition 10
(config)# vrf definition 20
(config)# vrf definition 30
```

VRF を L2 プロトコル併用無しで設定します。
<構築ポイント3.1.2-(1)>
(CSU 再起動を確認されますので、OK なら'y'を入力)

VRF10 を使用することを設定します。
VRF20 を使用することを設定します。
VRF30 を使用することを設定します。

VLAN の設定

```
(config)# vlan 2,10,20,31-32,100-101,200-201
```

使用する VLAN の設定をおこないます。

VLAN インタフェースの設定

```
(config)# interface vlan 2
(config-if)# ip address 172.255.0.1 255.255.0.0

(config)# interface vlan 10
(config-if)# vrf forwarding 10
(config-if)# ip address 10.0.0.1 255.255.0.0

(config)# interface vlan 20
(config-if)# vrf forwarding 20
(config-if)# ip address 20.0.0.1 255.255.0.0

(config)# interface vlan 31
(config-if)# vrf forwarding 31

(config)# interface vlan 32
(config-if)# vrf forwarding 32

(config)# interface vlan 100
(config-if)# vrf forwarding 10
(config-if)# ip address 192.168.0.1 255.255.255.0

(config)# interface vlan 101
(config-if)# vrf forwarding 10
(config-if)# ip address 192.168.1.1 255.255.255.0

(config)# interface vlan 200
(config-if)# vrf forwarding 20
(config-if)# ip address 192.168.0.1 255.255.255.0

(config)# interface vlan 201
(config-if)# vrf forwarding 20
(config-if)# ip address 192.168.1.1 255.255.255.0
```

VLAN2 はシステム管理用に global で使用します。
VLAN2 に IP アドレスを設定します。

VLAN10 はVRF10 で使用します。<構築ポイント3.1.2-(2)>
VLAN10 に IP アドレスを設定します。

VLAN20 はVRF20 で使用します。<構築ポイント3.1.2-(2)>
VLAN20 に IP アドレスを設定します。

VLAN31,VLAN32 はそれぞれ VRF31,VRF32 で使用しますが、IP アドレスは設定しません。

VLAN100 はVRF10 で使用します。<構築ポイント3.1.2-(2)>
VLAN100 に IP アドレスを設定します。

VLAN101 はVRF10 で使用します。<構築ポイント3.1.2-(2)>
VLAN101 に IP アドレスを設定します。

VLAN200 はVRF20 で使用します。<構築ポイント3.1.2-(2)>
VLAN200 に IP アドレスを設定します。

VLAN201 はVRF20 で使用します。<構築ポイント3.1.2-(2)>
VLAN200 に IP アドレスを設定します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

C1（AX6604S）の設定	
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface gigabitethernet 4/24 (config-if)# switchport access vlan 2	ポート 4/24 はシステム管理用に VLAN2 のアクセスポートとします。
(config)# interface range tengigabitethernet 1/1, tengigabitethernet 2/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 10 mode on	ポート 1/1,2/1 は装置 S1 接続用にチャネルグループ 10 を構成します。
(config)# interface range tengigabitethernet 1/3, tengigabitethernet 2/3 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on	ポート 1/3,2/3 はFW1 接続用にチャネルグループ 1 を構成します。<構築ポイント3.1.3-(3)>
(config)# interface range tengigabitethernet 1/4, tengigabitethernet 2/4 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 2 mode on	ポート 1/4,2/4 はFW2 接続用にチャネルグループ 2 を構成します。<構築ポイント3.1.3-(3)>
(config)# interface1 range gigabitethernet 3/1, gigabitethernet 4/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 11 mode on	ポート 3/1,4/1 は装置 A1 接続用にチャネルグループ 11 を構成します。
(config)# interface range gigabitethernet 3/2, gigabitethernet 4/2 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 12 mode on	ポート 3/2,4/2 は装置 A2 接続用にチャネルグループ 12 を構成します。
ポートチャネルの設定	
(config)# interface range port-channel 1-2 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,10,20,31-32	ポートチャネル 1 と 2 はトランクポートとし VLAN2,10,20,31-32 の転送を許可します。
(config)# interface port-channel 10 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,31-32	ポートチャネル 10 はトランクポートとし VLAN2,10,20,31-32 の転送を許可します。
(config)# interface port-channel 11 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,100-101	ポートチャネル 11 はトランクポートとし VLAN2,100-101 の転送を許可します。
(config)# interface port-channel 12 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,200-201	ポートチャネル 12 はトランクポートとし VLAN2,200-201 の転送を許可します。
デフォルトルートの設定	
(config)# ip route vrf10 0.0.0.0 0.0.0.0 172.16.0.254 (config)# ip route vrf20 0.0.0.0 0.0.0.0 172.16.0.254	VRF10 でのデフォルトルートを設定します。 VRF20 でのデフォルトルートを設定します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

(2) サーバ用アクセススイッチ（AX2530S)の設定

S1（AX2530S-24T4X）の設定	
スパニングツリーの抑止	
(config)# spanning-tree disable	AX シリーズではデフォルトで PVST+が有効になっており、FT 構成とする場合にはこれを抑止します。
VLAN の設定	
(config)# vlan 2,10,20,31-32	使用する VLAN の設定をおこないます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

S1（AX2530S-24T4X）の設定	
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.5 255.255.0.0	VLAN2 はシステム管理用に global で使用します。 VLAN2 に IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range tengigabitethernet 0/25-26 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on (config)# interface range gigabitethernet 0/1-4 (config-if-range)# switchport access vlan 10 (config)# interface range gigabitethernet 0/5-8 (config-if-range)# switchport access vlan 20 (config)# interface gigabitethernet 0/20 (config-if)# switchport access vlan 31 (config)# interface gigabitethernet 0/22 (config-if)# switchport access vlan 32	ポート 0/25-26 は装置 C1 接続用にチャネルグループ 1 を構成します。 ポート 0/1-4 は会社 A サーバ接続用に VLAN10 のアクセスポートとして構成します。 ポート 0/5-8 は会社 B サーバ接続用に VLAN20 のアクセスポートとして構成します。 ポート 0/20 は会社 A 外部接続用に VLAN31 のアクセスポートとして構成します。 ポート 0/22 は会社 B 外部接続用に VLAN32 のアクセスポートとして構成します。
ポートチャネルの設定	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,31-32	ポートチャネル 1 はトランクポートとし VLAN2,10,20,31-32 の転送を許可します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

(3) 端末PC用アクセススイッチ（AX1240S)の設定

A1（AX1240S-24T2C）の設定	
スパニングツリーの抑止	
(config)# spanning-tree disable	AX シリーズではデフォルトで PVST+が有効となっていますが、FT 構成とする場合はこれを抑止します。
VLAN の設定	
(config)# vlan 2,100-101	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.1.1 255.255.0.0	VLAN2 をシステム管理用に使用するため、装置の IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range gigabitethernet 0/25-26 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 11 mode on (config)# interface range fastethernet 0/1-12 (config-if-range)# switchport access vlan 100 (config)# interface fastethernet 0/13-24 (config-if-range)# switchport access vlan 101	ポート 0/25-26 は装置 C1,C2 接続用にチャネルグループ 11 を構成します。 VLAN2,100-101 のトランクポートとして構成します。 ポート 0/1-12 は会社 A 端末 PC のセグメント 1 接続用に VLAN100 のアクセスポートとして構成します。 ポート 0/13-24 は会社 A 端末 PC のセグメント 2 接続用に VLAN101 のアクセスポートとして構成します。
ポートチャネルの設定	
(config)# interface port-channel 11 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,100-101	ポートチャネル 11 はトランクポートとし VLAN2,100-101 の転送を許可します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

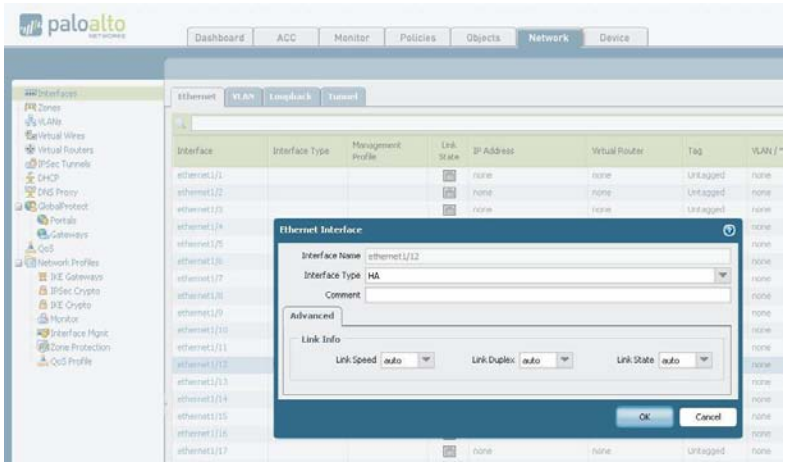
装置 B1 の設定は使用する VLAN ID と装置アドレスが異なる以外は装置 A1 の設定と同様です。
(VLAN：100-101→200-201、装置アドレス：172.255.1.1→172.255.2.1)

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(4) ファイアウォール(パロアルトネットワークスPAシリーズ)の設定

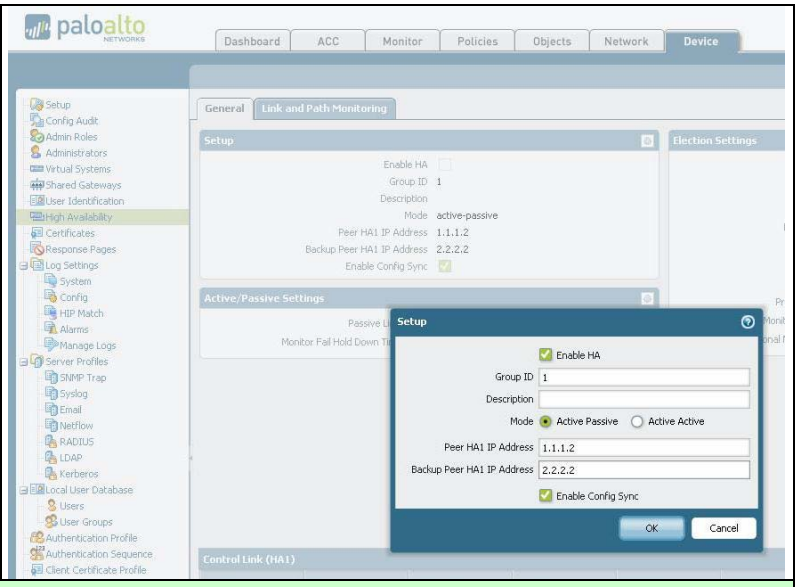
PA シリーズで HA 構成を組む場合、アクティブとする装置にて基本設定をおこなっておきます。

FW1 (PA-5060:アクティブ側) の設定 <構築ポイント3.1.3-(1)>

CLI	GUI
HA(冗長構成)の設定	
HA1 冗長接続用にEthernetインタフェースにHAインタフェースを設定 <構築ポイント3.1.3-(2)>	
`# set network interface ethernet ethernet1/12 ha`	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** Interface – ethernet1/12 選択で Ethernet Interface 設定ウインドウ [Interface Type] HA <OK> 
HA を設定	

`# set deviceconfig high-availability enabled yes`
 	
`# set deviceconfig high-availability group 1 mode active-passive`
 	
`# set deviceconfig high-availability group 1 peer-ip 1.1.1.2`
 	
`# set deviceconfig high-availability group 1 peer-ip-backup 2.2.2.2`
 	
`# set deviceconfig high-availability group 1 configration-synchronization enabled yes`
 	
`# set deviceconfig high-availability group 1 election-option device-priority 10`
 	
`# set deviceconfig high-availability interface ha1 port dedicated-ha1 ip-address 1.1.1.1 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha1-backup port ethernet1/12 ip-address 2.2.2.1 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha2 port dedicated-ha2`
	[Device]＞[High Availability]＞[General]タブ画面
	・Setup 設定ウインドウ
	[Enable HA]にチェック
	[Group ID] 1
	[Mode] Active Passive
	[Peer HA1 IP Address] 1.1.1.2
	[Backup Peer HA1 IP Address] 2.2.2.2
	[Enable Config Sync]にチェック
	<OK>
	
	・Election Settings設定ウインドウ <構築ポイント3.1.3-(3)>
	[Device Priority] 10
	<OK>
	
	・Control Link(HA1) – Primary 設定ウインドウ
	[Port] dedicated-ha1(Dedicated out of band HA1 interface)
	[IP Address] 1.1.1.1
	[Netmask] 255.255.255.0
	<OK>
	
	・Control Link(HA1) – Backup設定ウインドウ <構築ポイント3.1.3-(2)>
	[Port] ethernet1/12
	[IP Address] 2.2.2.1
	[Netmask] 255.255.255.0
	<OK>
	・Data Link(HA2)設定 – Primary 設定ウインドウ
	[Port] dedicated-ha2(Dedicated out of band HA2 interface)
	<OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.



リンクモニタリングの設定

```
#set deviceconfig high-availability
group 1 monitoring link-monitoring
link-group toAX interface [ ethernet1/23
ethernet1/24 ]

#set deviceconfig high-availability
group 1 monitoring link-monitoring
link-group toAX enabled yes

#set deviceconfig high-availability
group 1 monitoring link-monitoring
link-group toAX failure-condition all
```

[Device]＞[High Availability]＞[Link and Path Monitoring]タブ画面

・[Link Group]にて[Add] – Link Group 設定ウインドウ

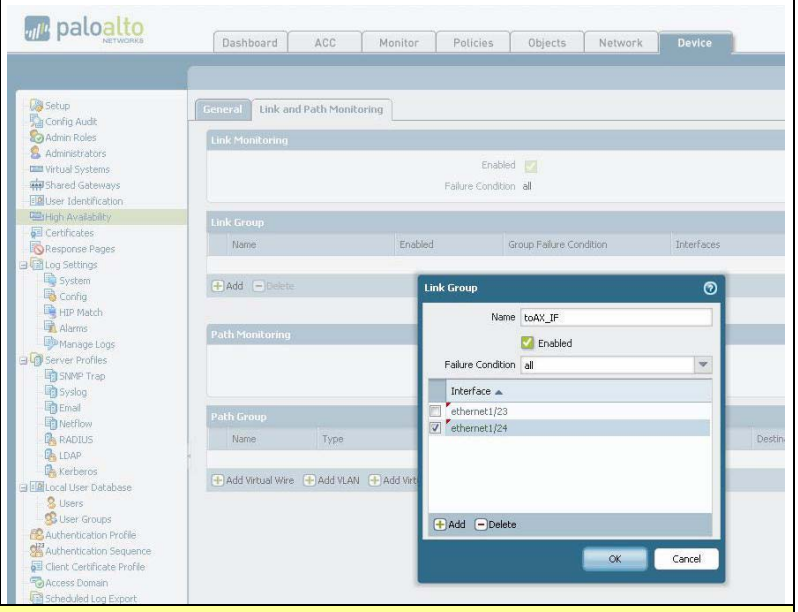
[Name] toAX

[Enabled]にチェック

[Failure Condition] all

[Interfaces▲] ethernet1/23, ethernet1/24 を Add

<OK>



バーチャルシステム(VSYS)使用の設定

バーチャルシステムの使用を設定し、commitして設定を反映 **<構築ポイント3.1.3-(9)>**

※一旦quitしオペレーショナルモードより設定

```
> set  system setting multi-vsys on
> configure

# commit
```

[Device]＞[Setup]＞[Management]タブ画面

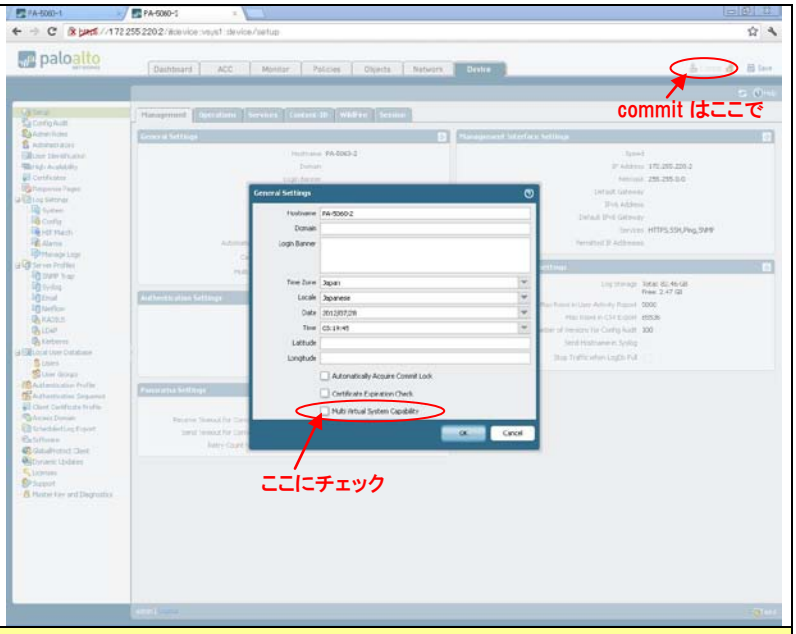
・General Settings 設定ウインドウ

[Multi Virtual System Capability]にチェック

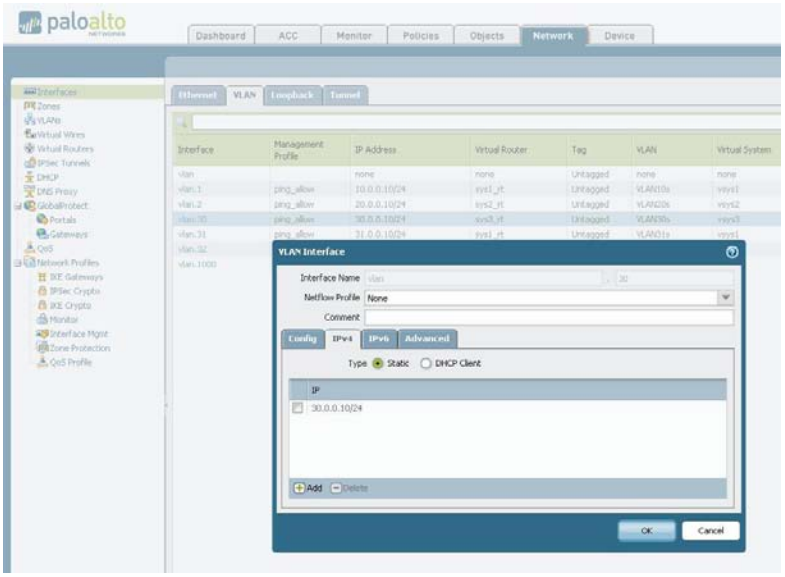
<OK>

画面右上 Commit をクリック

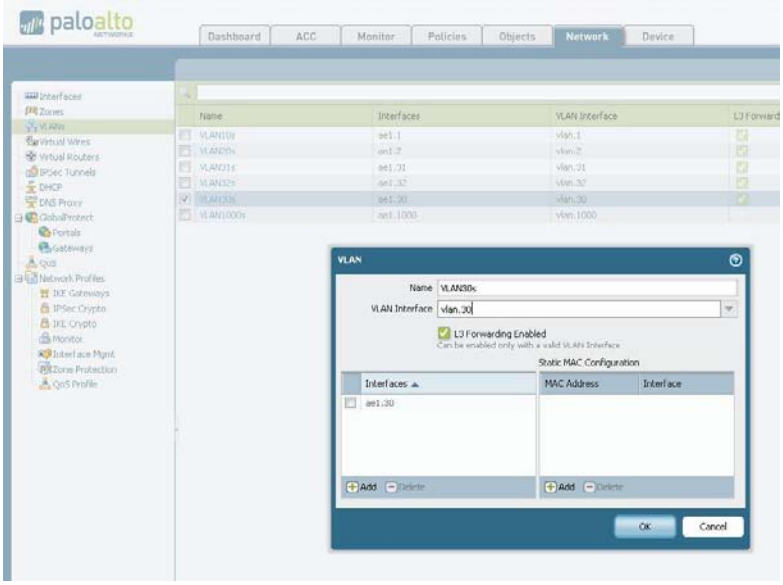
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

	
インタフェースの設定	
Aggregate Ethernetインタフェース作成および設定 <構築ポイント3.1.3-(5)>	
#set network interface aggregate-ethernet ae1 layer2	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** ・[Add Aggregate Group]で AggregateGroup 設定ウインドウ [Interface name] ae 1 <OK>
#set network interface ethernet ethernet1/23 aggregate-group ae1	・Interface – ethernet1/23 選択で Ethernet Interface 設定ウインドウ [Interface name] ae1 [Interface Type] Aggregate Ethernet <OK>
#set network interface ethernet ethernet1/24 aggregate-group ae1	・Interface – ethernet1/24 選択で Ethernet Interface 設定ウインドウ [Interface name] ae1 [Interface Type] Aggregate Ethernet <OK>
タグ付きインタフェース(Layer2 Subinterface)作成および設定	
#set network interface aggregate-ethernet ae1 layer2 units ae1.1 tag 10	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** ・[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　1　*(Interface 名=ae1.1 となる)* [Tag] 10 <OK>
#set network interface aggregate-ethernet ae1 layer2 units ae1.2 tag 20	・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　2　*(Interface 名=ae1.2 となる)* [Tag] 20 <OK>
#set network interface aggregate-ethernet ae1 layer2 units ae1.31 tag 31	・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　31　*(Interface 名=ae1.31 となる)* [Tag] 31 <OK>
#set network interface aggregate-ethernet ae1 layer2 units ae1.32 tag 32	・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　32　*(Interface 名=ae1.32 となる)* [Tag] 32 <OK>
#set network interface aggregate-ethernet ae1 layer2 units ae1.9002 tag 2	・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　9002　*(Interface 名=ae1.9002 となる)* [Tag] 2 <OK>

Copyright © 2013,　ALAXALA Networks Corporation. All rights reserved.

VLAN インタフェースの作成と設定	
#set network interface vlan units vlan.1 ip 10.0.0.10/24	**[Network]＞[Interfaces]＞[VLAN]タブ画面** ・[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 1 *（VLAN Interface 名=vlan.1 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 10.0.0.10/24 〈OK〉
#set network interface vlan units vlan.2 ip 20.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 2 *（VLAN Interface 名=vlan.2 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 20.0.0.10/24 〈OK〉
#set network interface vlan units vlan.31 ip 31.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 31 *（VLAN Interface 名=vlan.31 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 31.0.0.10/24 〈OK〉
#set network interface vlan units vlan.32 ip 32.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 32 *（VLAN Interface 名=vlan.32 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 32.0.0.10/24 〈OK〉
#set network interface vlan units vlan.9002 ip 172.255.0.10/16	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 9002 *（VLAN Interface 名=vlan.9002 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 172.255.0.10/16 〈OK〉 

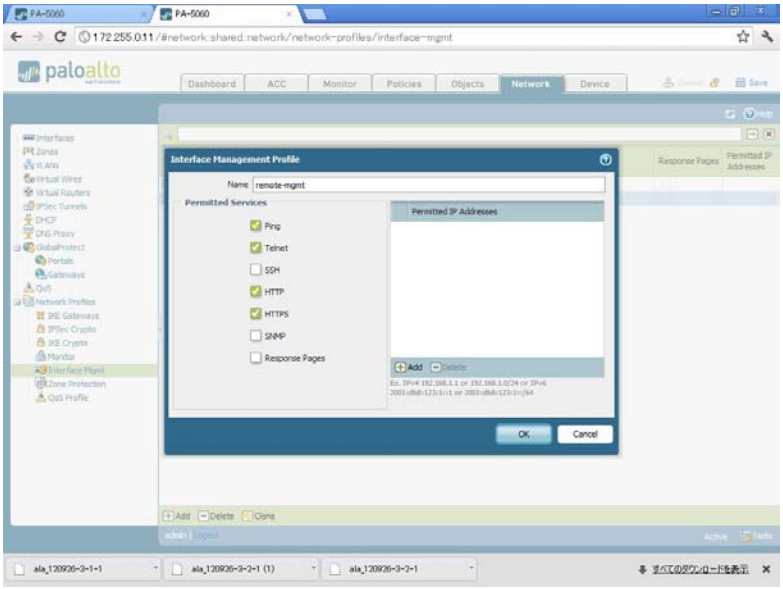
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

VLAN の作成	
#set network vlan VLAN10s interface ae1.1 virtual-interface interface vlan.1 l3-forwarding yes	**[Network]＞[VLANs]タブ画面** ・[Add]で VLAN 設定ウインドウ [Name] VLAN10s [VLAN Interface] vlan.1 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.1 を Add 〈OK〉
#set network vlan VLAN20s interface ae1.2 virtual-interface interface vlan.2 l3-forwarding yes	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN20s [VLAN Interface] vlan.2 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.2 を Add 〈OK〉
#set network vlan VLAN31s interface ae1.31 virtual-interface interface vlan.31 l3-forwarding yes	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN31s [VLAN Interface] vlan.31 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.31 を Add 〈OK〉
#set network vlan VLAN32s interface ae1.32 virtual-interface interface vlan.32 l3-forwarding yes	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN32s [VLAN Interface] vlan.32 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.32 を Add 〈OK〉
#set network vlan MGT-VLAN interface ae1.9002 virtual-interface interface vlan.9002	・再度[Add]で VLAN 設定ウインドウ [Name] MGT-VLAN [VLAN Interface] vlan.9002 [Interfaces▲] ae1.9002 を Add 〈OK〉
	

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

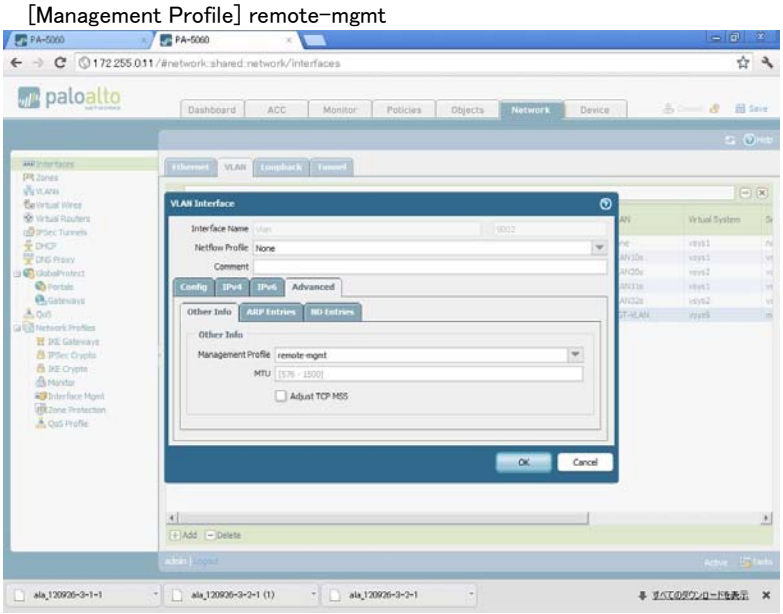
<table>
<tr><td colspan="2">Layer3 インタフェース用管理プロファイルの設定 <構築ポイント3.1.3-(7)></td></tr>
<tr><td colspan="2">装置のリモート管理用プロファイルの設定</td></tr>
<tr><td>

```
#set network profiles
interface-management-profile
remote-mgmt ping yes telnet yes http yes
https yes
```

</td><td>
[Network]＞[Network Profiles]-[Interface mgmt] 画面
・[Add]で Interface Management Profile 設定ウインドウ
[Name] remote-mgmt
Permitted Services 内の[Ping][Telnet][HTTP][HTTPS]等、
必要な項目にチェック
[Permitted IP Address] 必要に応じて、許可するホストまたは
ネットワークアドレスを追加
<OK>


</td></tr>
<tr><td>

```
#set network interface vlan units
vlan.9002 interface-management-profile
remote-mgmt
```

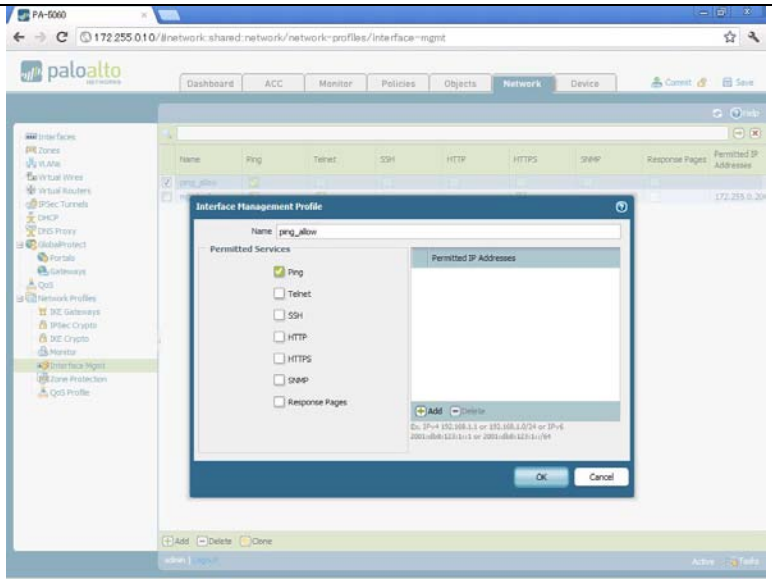
</td><td>
[Network]＞[Interfaces]＞[VLAN]タブ画面
・[Interface]以下 vlan.9002 を選択で VLAN interface 設定ウインドウ
Advanced タブ-OtherInfo タブ
[Management Profile] remote-mgmt


</td></tr>
<tr><td colspan="2">Layer3 インタフェースを ping 応答可とする設定（必要に応じて）</td></tr>
<tr><td>

```
#set network profiles
interface-management-profile
ping_allow ping yes
```

</td><td>
[Network]＞[Network Profiles]-[Interface mgmt] 画面
・[Add]で Interface Management Profile 設定ウインドウ
[Name] ping_allow
Permitted Services 内の[Ping]にチェック
<OK>
</td></tr>
</table>

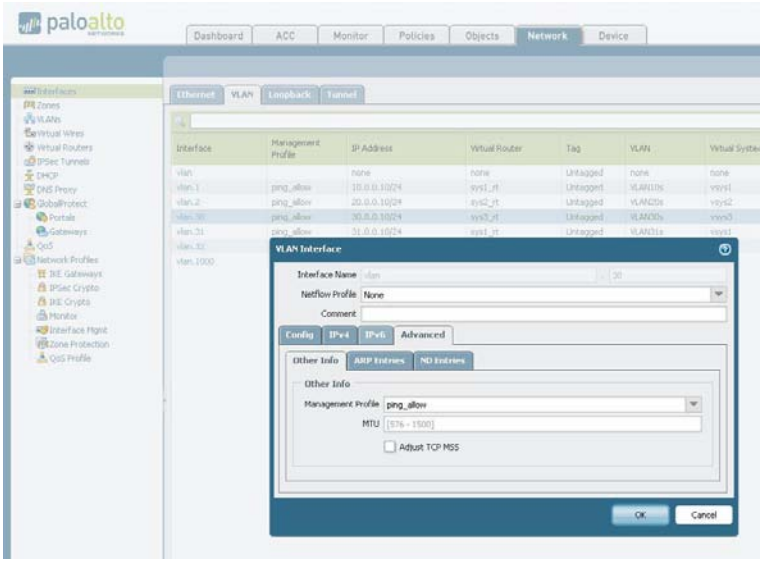
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.



この設定以降、Layer3 としたインタフェースの[Advanced]-[Other Info]タブ以下で[Management Profile]で ping_allow が選択できるようになるため、ping 応答させたい Layer3 インタフェースで適宜選択する。

(vlan.31への設定例)

```
#set network interface vlan units
vlan.31 interface-management-profile
ping_allow
```



VSYS1 (会社 A 用ファイアウォール)の設定

VSYS を作成

```
#delete vsys vsys1 import network
interface ethernet1/12

#set vsys vsys1 import network interface
[ ae1.1 ae1.31 vlan.1 vlan.31 ]
```

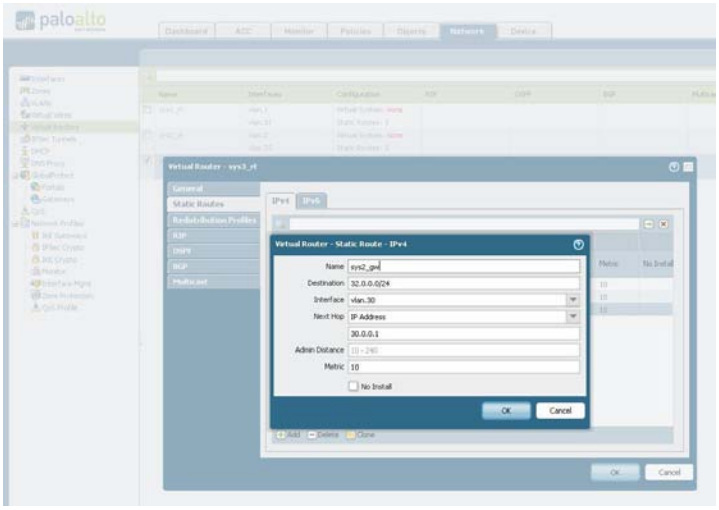
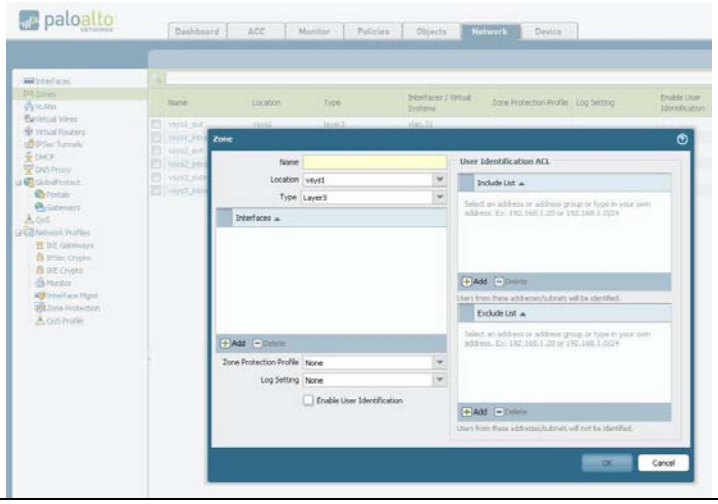
[Device]>[Virtual Systems] 画面
・[Add]で vsys 設定ウインドウ
[ID] 1
General タブ - [Interfaces▲] ae1.1, ae1.31, vlan.1, vlan.31 を add
<OK>

仮想ルータを設定 <構築ポイント3.1.3-(6)>

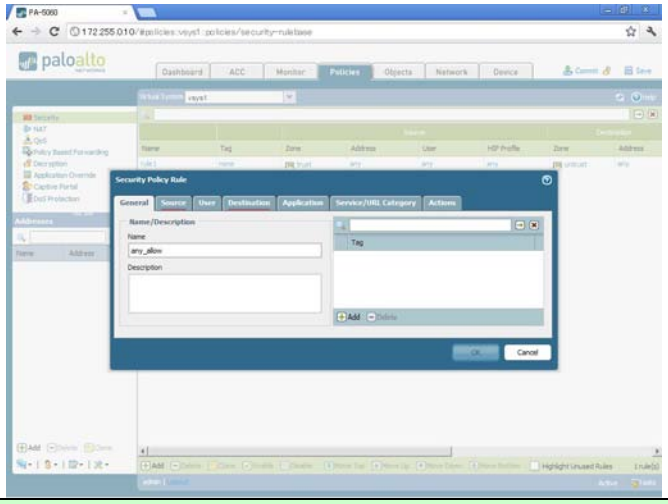
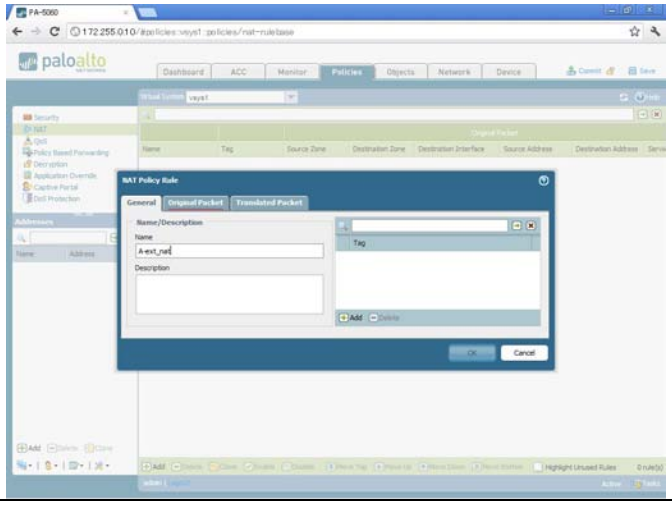
```
#set network virtual-router sys1_rt
interface [ vlan.1 vlan.31 ]
routing-table ip static-route default
destination 0.0.0.0/0 nexthop
ip-address 31.0.0.254
```

[Network]>[Virtual Routers] 画面
・[Add]で Virtual Router 設定ウインドウ
General タブ
[Name] sys1_rt
[Interfaces▲] vlan.1, vlan.31 を Add
Static Routes タブ - IPv4 タブ
[Add]で Virtual Router - Static Route - IPv4 設定ウインドウ
[Name] default
[Destination] 0.0.0.0/0
[Next Hop] IP Address を選択し、下の行に 31.0.0.254 入力
<OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

#set network virtual-router sys1_rt routing-table ip static-route A-TERM1 destination 192.168.0.0/24 nexthop ip-address 10.0.0.1 #set network virtual-router sys1_rt routing-table ip static-route A-TERM2 destination 192.168.1.0/24 nexthop ip-address 10.0.0.1	再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] A-TERM1 [Destination] 192.168.0.0/24 [Next Hop] IP Address を選択し、下の行に 10.0.0.1 入力 <OK> 再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] A-TERM2 [Destination] 192.168.1.0/24 [Next Hop] IP Address を選択し、下の行に 10.0.0.1 入力 <OK> <OK> 
#set vsys vsys1 import network virtual-router sys1_rt	**[Device]＞[Virtual Systems] 画面** ・vsys1 を選択 General タブ – [Virtual Routers▲] sys1_rt を add <OK>
ゾーンを設定 〈構築ポイント3.1.3-(6)〉	
#set vsys vsys1 zone vsys1_trust network layer3 vlan.1 #set vsys vsys1 zone vsys1_untrust network layer3 vlan.31	**[Network]＞[Zones] 画面** ・[Add]で Zone 設定ウインドウ [Name] vsys1_trust [Location] vsys1 [Type] Layer3 [Interfaces▲] vlan.1 を add <OK> ・再度[Add]で Zone 設定ウインドウ [Name] vsys1_untrust [Location] vsys1 [Type] Layer3 [Interfaces▲] vlan.31 を add <OK> 

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

セキュリティ(フィルタ)を設定	
#set vsys vsys1 rulebase security rules any_allow from any to any #set vsys vsys1 rulebase security rules any_allow source any destination any #set vsys vsys1 rulebase security rules any_allow application any service any action allow	**[Policies]＞[Security] 画面** – [Virtual System] vsys1 選択 ・[Add]で Security Policy Rule 設定ウインドウ General タブ [Name] any_allow Source タブ Source Zone および Source Address の上の[Any]にチェック Destination タブ Destination Zone の上[Any]選択 Destination Address の上[Any]にチェック Actions タブ Action Setting [Action] allow <OK> 
NAT ポリシーの追加	
#set vsys vsys1 rulebase nat rules A-ext_nat to vsys1_untrust from vsys1_trust #set vsys vsys1 rulebase nat rules A-ext_nat source any destination any service any #set vsys vsys1 rulebase nat rules A-ext_nat source-translation dynamic-ip-and-port interface-address interface vlan.31	**[Policies]＞[NAT] 画面** – [Virtual System] vsys1 選択 ・[Add]で NAT Policy Rule 設定ウインドウ General タブ [Name] A-ext_nat Original Packet タブ [Source Zone] vsys1_trust を Add [Destination Zone] vsys1_untrust [Service] Any [Source Address] Any にチェック [Destination Address] Any にチェック Translated Packet タブ [Translation Type] Dynamic IP and Port [Address Type] Interface Address [Interface] vlan.31 [IP Adress] 31.0.0.10/24 <OK> 

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

VSYS2（会社 B 用ファイアウォール）の設定	
VSYS を作成	
#set vsys vsys2 import network interface [ae1.2 ae1.32 vlan.2 vlan.32]	**[Device]＞[Virtual Systems] 画面** ・[Add]で vsys 設定ウインドウ [ID] 2 General タブ – [Interfaces▲] ae1.2, ae1.32, vlan.2, vlan.32 を add 〈OK〉
仮想ルータを設定 〈構築ポイント3.1.3-(6)〉	
#set network virtual-router sys2_rt interface [vlan.2 vlan.32] routing-table ip static-route default destination 0.0.0.0/0 nexthop ip-address 32.0.0.254 #set network virtual-router sys2_rt routing-table ip static-route B-TERM1 destination 192.168.0.0/24 nexthop ip-address 20.0.0.1 #set network virtual-router sys2_rt routing-table ip static-route B-TERM2 destination 192.168.1.0/24 nexthop ip-address 20.0.0.1 #set vsys vsys2 import network virtual-router sys2_rt	**[Network]＞[Virtual Routers] 画面** ・[Add]で Virtual Router 設定ウインドウ General タブ [Name] sys2_rt [Interfaces▲] vlan.2 vlan.32 を Add Static Routes タブ – IPv4 タブ [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] default [Destination] 0.0.0.0/0 [Next Hop] IP Address を選択し、下の行に 32.0.0.254 入力 〈OK〉 再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] B-TERM1 [Destination] 192.168.0.0/24 [Next Hop] IP Address を選択し、下の行に 20.0.0.1 入力 〈OK〉 再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] B-TERM2 [Destination] 192.168.1.0/24 [Next Hop] IP Address を選択し、下の行に 20.0.0.1 入力 〈OK〉 〈OK〉 **[Device]＞[Virtual Systems] 画面** ・vsys2 を選択 General タブ – [Virtual Routers▲] sys2rt を add 〈OK〉
ゾーンを設定 〈構築ポイント3.1.3-(6)〉	
#set vsys vsys2 zone vsys2_trust network layer3 vlan.2 #set vsys vsys2 zone vsys2_untrust network layer3 vlan.32	**[Network]＞[Zones] 画面** ・[Add]で Zone 設定ウインドウ [Name] vsys2_trust [Location] vsys2 [Type] Layer3 [Interfaces▲] vlan.2 を add 〈OK〉 ・再度[Add]で Zone 設定ウインドウ [Name] vsys2_untrust [Location] vsys2 [Type] Layer3 [Interfaces▲] vlan.32 を add 〈OK〉
セキュリティ(フィルタ)を設定	
#set vsys vsys2 rulebase security rules any_allow from any to any #set vsys vsys2 rulebase security rules any_allow source any destination any #set vsys vsys2 rulebase security rules any_allow application any service any action allow	**[Policies]＞[Security] 画面** – [Virtual System] vsys2 選択 ・[Add]で Security Policy Rule 設定ウインドウ General タブ [Name] any_allow Source タブ Source Zone および Source Address の上の[Any]にチェック Destination タブ Destination Zone の上[Any]選択 Destination Address の上[Any]にチェック Actions タブ Action Setting [Action] allow 〈OK〉

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

NAT ポリシーの追加	
#set vsys vsys2 rulebase nat rules B-ext_nat to vsys2_untrust from vsys2_trust #set vsys vsys2 rulebase nat rules B-ext_nat source any destination any service any #set vsys vsys2 rulebase nat rules B-ext_nat source-translation dynamic-ip-and-port interface-address interface vlan.32	**[Policies]＞[NAT] 画面** – [Virtual System] vsys2 選択 ・[Add]で NAT Policy Rule 設定ウインドウ General タブ [Name] B-ext_nat Original Packet タブ [Source Zone] vsys2_trust を Add [Destination Zone] vsys2_untrust [Service] Any [Source Address] Any にチェック [Destination Address] Any にチェック Translated Packet タブ [Translation Type] Dynamic IP and Port [Address Type] Interface Address [Interface] vlan.32 [IP Adress] 32.0.0.10/24 <OK>
VSYS9 (システム管理用 VSYS)の設定	
VSYS を作成	
#set vsys vsys9 import network interface [ae1.9002 vlan.9002]	**[Device]＞[Virtual Systems] 画面** ・[Add]で vsys 設定ウインドウ [ID] 9 General タブ – [Interfaces▲] ae1.9002, vlan.9002 を add <OK>
仮想ルータを設定 <構築ポイント3.1.3-(6)>	
#set network virtual-router sys2_rt interface [vlan.9002] #set vsys vsys9 import network virtual-router mgt_rt	**[Network]＞[Virtual Routers] 画面** ・[Add]で Virtual Router 設定ウインドウ General タブ [Name] mgt_rt [Interfaces▲] vlan.9002 を Add <OK> **[Device]＞[Virtual Systems] 画面** ・vsys9 を選択 General タブ – [Virtual Routers▲] mgt_rt を add <OK>
ゾーンを設定 <構築ポイント3.1.3-(6)>	
#set vsys vsys9 zone mgt-zone network layer3 vlan.9002	**[Network]＞[Zones] 画面** ・[Add]で Zone 設定ウインドウ [Name] mgt-zone [Location] vsys9 [Type] Layer3 [Interfaces▲] vlan.9002 を add <OK>
セキュリティ(フィルタ)を設定	
#set vsys vsys9 rulebase security rules any_allow from any to any #set vsys vsys9 rulebase security rules any_allow source any destination any #set vsys vsys9 rulebase security rules any_allow application any service any action allow	**[Policies]＞[Security] 画面** – [Virtual System] vsys9 選択 ・[Add]で Security Policy Rule 設定ウインドウ General タブ [Name] any_allow Source タブ Source Zone および Source Address の上の[Any]にチェック Destination タブ Destination Zone の上[Any]選択 Destination Address の上[Any]にチェック Actions タブ Action Setting [Action] allow <OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

VSYS管理ユーザの追加（必要に応じて） <構築ポイント3.1.3-(8)>

VSYS1 管理ユーザの追加

```
#set mgt-config users sys1-admin
permissions role-based vsysadmin
localhost.localdomain vsys vsys1

#set mgt-config users sys1-admin password
Enter password   : sys1-admin用パスワード
Confirm password : もう一度パスワード入力
```

[Device]＞[Administrators] 画面

・[Add]で Administrator 設定ウインドウ

[Name] sys1-admin

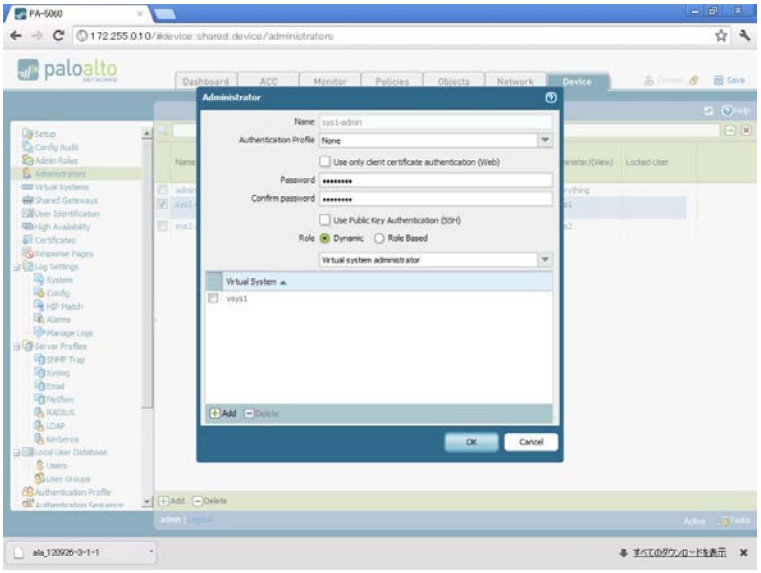
[Password] *sys1-admin 用パスワード*

[Confirm password] *もう一度パスワード入力*

[Virtual system administrator]を選択

[Virtual System] vsys1 を Add

<OK>



設定内容の反映 <構築ポイント3.1.3-(9)>

```
# commit
```

画面右上 Commit をクリック

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

続いて、パッシブとして使用する装置の設定をマスタ装置と接続する前に以下のように設定します。

FW2 (PA-5060:パッシブ側) の設定	
CLI	**GUI**
HA の設定	
HA1 冗長接続用に Ethernet インタフェースに HA インタフェースを設定	
`# set network interface ethernet ethernet1/12 ha`	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** Interface – ethernet1/12 選択で Ethernet Interface 設定ウインドウ [Interface Type] HA <OK>
HA を設定	

`# set deviceconfig high-availability enabled yes`
 	
`# set deviceconfig high-availability group 1 mode active-passive`
 	
`# set deviceconfig high-availability group 1 peer-ip 1.1.1.1`
 	
`# set deviceconfig high-availability group 1 peer-ip-backup 2.2.2.1`
 	
`# set deviceconfig high-availability group 1 configration-synchronization enabled yes`
 	
`# set deviceconfig high-availability group 1 election-option device-priority 10`
 	
`# set deviceconfig high-availability interface ha1 port dedicated-ha1 ip-address 1.1.1.2 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha1-backup port ethernet1/12 ip-address 2.2.2.2 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha2 port dedicated-ha2`
	[Device]＞[High Availability]＞[General]タブ画面
	・Setup 設定ウインドウ
	[Enable HA]にチェック
	[Group ID] 1
	[Mode] Active Passive
	[Peer HA1 IP Address] 1.1.1.1
	[Backup Peer HA1 IP Address] 2.2.2.1
	[Enable Config Sync]にチェック
	<OK>
	
	・Election Settings 設定ウインドウ
	[Device Priority] 10
	<OK>
	
	・Control Link(HA1) – Primary 設定ウインドウ
	[Port] dedicated-ha1(Dedicated out of band HA1 interface)
	[IP Address] 1.1.1.2
	[Netmask] 255.255.255.0
	<OK>
	
	・Control Link(HA1) – Backup 設定ウインドウ
	[Port] ethernet1/12
	[IP Address] 2.2.2.2
	[Netmask] 255.255.255.0
	<OK>
	
	・Data Link(HA2)設定 – Primary 設定ウインドウ
	[Port] dedicated-ha2(Dedicated out of band HA2 interface)
	<OK>

リンクモニタリングの設定	

`#set deviceconfig high-availability group 1 monitoring link-monitoring link-group toAX interface [ ethernet1/23 ethernet1/24 ]`
 	
`#set deviceconfig high-availability group 1 monitoring link-monitoring link-group toAX enabled yes`
 	
`#set deviceconfig high-availability group 1 monitoring link-monitoring link-group toAX failure-condition all`
	[Device]＞[High Availability]＞[Link and Path Monitoring]タブ画面
	・[Link Group]にて[Add] – Link Group 設定ウインドウ
	[Name] toAX
	[Enabled]にチェック
	[Failure Condition] all
	[Interfaces▲] ethernet1/23, ethernet1/24 を Add
	<OK>

設定内容の反映	
`# commit`	画面右上  をクリック

以上の設定終了後、アクティブ装置へ接続します。

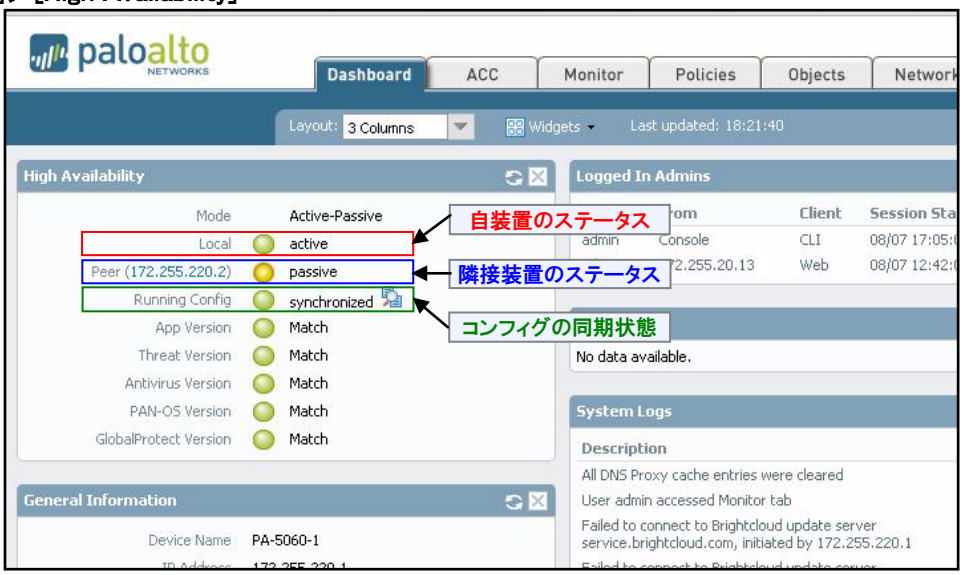
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

パッシブ側の装置については、アクティブ側の装置でおこなった設定をおこなう必要はなく、アクティブ装置とコンフィグの同期をおこなえば OK です。

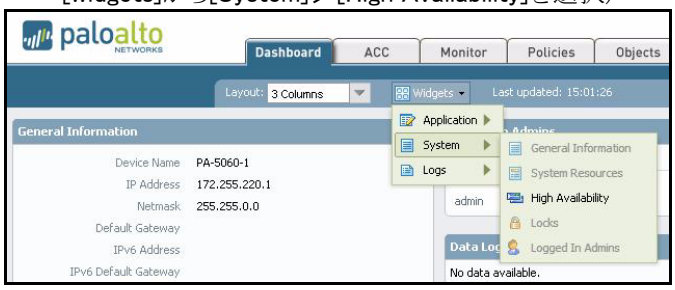
FW1（PA-5060：アクティブ側）の設定	
CLI	GUI
HAの同期 <構築ポイント3.1.3-(5)>	
実行コンフィグの同期	
> request high-availability sync-to-remote running-config	[Dashboard]タブ＞[HighAvailability]ウィジェット [Running Config]の項、sync to peer 横の Sync to peer をクリック

HA の状態確認は以下の通りです。

GUI の場合
[Dashboard]＞[High Availability]



※[Dashboard]に[High Availability]ウィジェットが無い場合は、
[widgets]から[System]＞[High Availability]を選択）



Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

CLI の場合

```
# show high-availability state

Group 1:
  Mode: Active-Passive
  Local Information:                                          自装置の情報
    Version: 1
    Mode: Active-Passive
    State: active                                             自装置のステータス
    Device Information:
      Management IP Address: 172.255.0.10; Netmask: 255.255.0.0
      Jumbo-Frames disabled; MTU 1500
    HA1 Control Links Joint Configuration:
      Encryption Enabled: no
    Election Option Information:
      Priority: 10
      Preemptive: no
    Version Compatibility:
      Software Version: Unknown
      Application Content Compatibility: Unknown
      Threat Content Compatibility: Unknown
      Anti-Virus Compatibility: Unknown
      VPN Client Software Compatibility: Unknown
      Global Protect Client Software Compatibility: Unknown
    State Synchronization: not synchronized; type: ethernet
  Peer Information:                                           隣接装置の情報
    Connection status: down                                   隣接装置の接続状況
    Connection down reason: Never able to connect to peer
    Version: 0
    Mode: Unknown
    State: unknown                                            隣接装置のステータス
    Device Information:
      Management IP Address:
      Connection down; Reason: Never able to connect to peer
      Connection down; Reason: Never able to connect to peer
    Election Option Information:
      Priority: 100
      Preemptive: no
  Configuration Synchronization:
    Enabled: yes
    Running Configuration: unknown                            コンフィグの同期状態
```

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.2 組織単位に分割管理する場合の適用例（スタック構成+PAシリーズHA構成）

企業など、既にネットワークを一つの大きな単位で使用しているケースで、1 章での解説のようにセキュリティ管理を強化するために、ネットワークの単位を組織ごとに細分化する例について解説します。

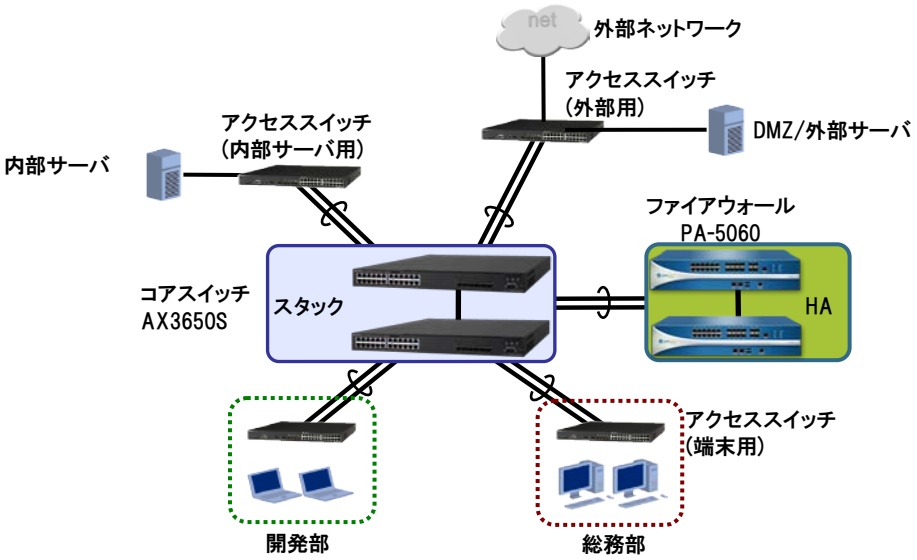


図 3.2-1 部門別仮想ネットワーク物理構成

物理構成は以上のように単一のシステムを構成した場合とほとんど変わらない構成となります。しかしながら、仮想ネットワークを含めた論理的なネットワーク構成は以下の通りとなります。ファイアウォールについては、PA-5060 を冗長構成で使用しネットワークのコア部分に組み込む形となります。

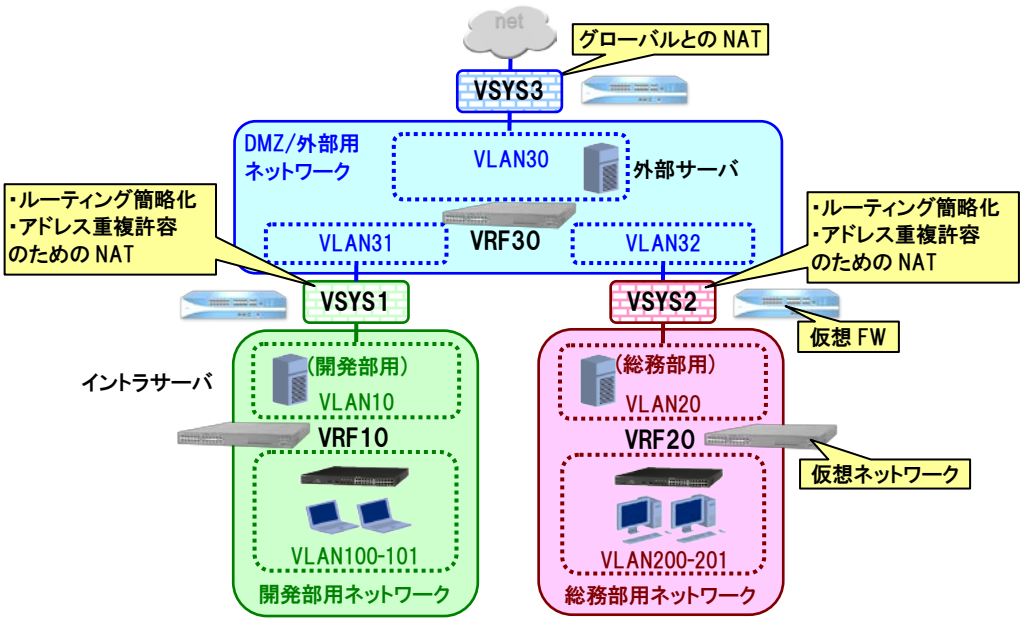


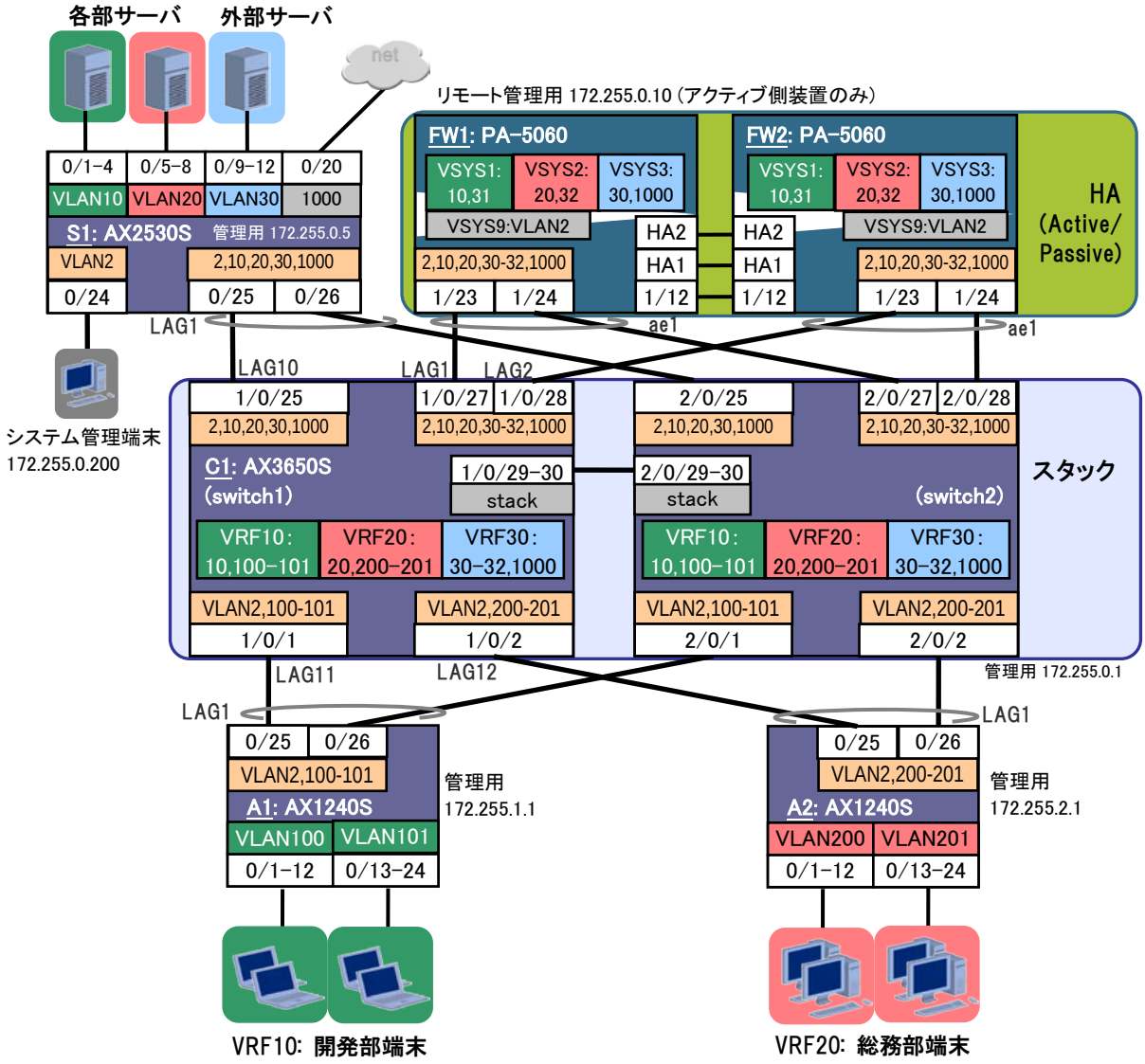
図 3.2-2 部門別仮想ネットワーク論理構成

ネットワーク・パーティション(VRF)による仮想ネットワークにて、開発部、総務部それぞれを独立した L3 ネットワークとし、また DMZ として使用する外部接続用のセグメントも仮想ネットワークとして、独立したネットワークとします。そしてそれぞれを仮想ファイアウォール(VSYS)にて橋渡しするように構成します。

これにより、開発部および総務部それぞれ独立したネットワークでの構成となり、また各部門の脅威管理(アンチウイルス、IPS、各種フィルタ)を含めたアクセス管理も各 VSYS で独立しておこなうことが可能となります。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

また、装置個別の設定を反映した論理構成は以下の通りとなります。



用途	VSYS	VRF ID	VLAN ID	IP アドレス(*1)
外部接続用	VSYS3	30	1000	100.0.0.0/24 (外部ルータ: .254)
			30	30.0.0.0/24
開発-外部接続用	VSYS1		31	31.0.0.0/24
開発部サーバ/Uplink 用		10	10	10.0.0.10/24
開発部端末 PC 用	-		100-101	192.168.0-1.0/24
総務-外部接続用	VSYS2	30	32	32.0.0.0/24
総務部サーバ/Uplink 用		20	20	20.0.0.10/24
総務部端末 PC 用	-		200-201	192.169.0-1.0/24
システム総合管理用	VSYS9	global	2	172.255.0.0/16

(*1) ホストアドレス x.x.x.1 は装置 C1 で、x.x.x.10 は装置 FW1/FW2 で使うものとする。

図 3.2-3 部門別仮想ネットワーク 論理設定詳細

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.2.1 システム構築時のポイント

本例の構成を設計する際におけるポイントを以下に示します。

(1) コアスイッチ、ファイアウォールの要求性能や収容条件は、もとのシステムで使用の装置と同等で良い。

今回の構成のように、もととなるネットワークで VLAN にてセグメント分けしていた部分を、仮想ネットワークで置き換えるといった構成とする場合、ネットワーク全体の収容条件はもとのネットワークとほとんど変わらないこととなります。従って使用する装置の選定に関しては、もとのネットワークで使用していた装置の収容条件と同等と考えることができます。

(2) 可用性の確保はスタック構成を基本とし、ファイアウォール(PAシリーズ)はHA構成とする。

コアスイッチが AX3650S である場合、障害などに対する可用性の確保のために 2 台をスタック構成として構築します。PA シリーズも同様に 2 台以上を用意し、装置冗長構成の機能である HA を用います。

(3) コアスイッチとファイアウォール間はスタティックリンクアグリゲーションにて接続する。

コアスイッチとファイアウォール間の接続については、リンクアグリゲーション(PA シリーズでは Aggregate Ethernet インタフェースと呼びます。)を用いて回線の可用性を確保します。

(4) 各VSYSでNATを使用すれば、IPアドレスの重複も可能。

VSYS は仮想のファイアウォールとして機能しますが、各 VSYS では NAT も各々独立して機能します。このため、各部門で使用する IP アドレスを重複させることが可能です。

また、部門ごとの仮想ネットワーク(VRF10,VRF20)が接続される外部接続用の仮想ネットワーク(VRF30)内でのルーティングテーブルも簡略化することが可能です。

ただし、同じ PA シリーズで NAT を複数回繰り返すことになり、システム全体として見たときの転送性能の上限が小さくなる、レイテンシが大きくなるなど、システム全体のパフォーマンスにも影響があるため注意が必要です。

(5) PAシリーズはインターネットと接続できるパスを設ける。

PA シリーズのライセンス管理や各種フィルタ機能で使用されるパターンファイル、シグネチャ等の更新などは外部にある専用サーバを通しておこないます。従って PA シリーズはインターネット接続できる環境下に置く必要があります。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.2.2 スイッチ(AXシリーズ)設定時のポイント

コンフィグなど、機器の設定の際のポイントを以下に示します。

(1) スタック機能を使用する。 AX Serise

AX3650S シリーズにてコアスイッチを構成する場合、使用できる機能などが許される限り、スタック構成での使用を推奨します。スタック構成とすることで、ボックススイッチでも FT スイッチと同等な高可用性を持つシステムを構築することができます。

AX シリーズでのスタック構成の設定ポイントや設定方法については、「AX シリーズ スタック導入ガイド」に詳しいため、スタックの構成にあたってはそちらも一読されることを推奨いたします。

(2) ボックス型(AX3650S)でVRFを使用する場合、モードの設定は不要 AX Serise

AX3650S で VRF 機能を使用する場合、VRF モードの設定は不要です。また VRF モード設定に伴うスイッチング機構の再起動等もありません。

(3) VLANインタフェースでの設定は最初に所属VRFの設定からおこなう。 AX Serise

VLAN インタフェースでは、所属 VRF の設定と IP アドレスの設定が必要ですが、所属 VRF の設定は IP アドレスの設定前におこなう必要があります。(IP アドレスが設定されている状態では所属 VRF の設定はできません。)

ですので、VLAN インタフェースの設定では所属 VRF の設定を最初におこなってください。

(4) PAシリーズとの接続もリンクアグリゲーションで接続 AX Serise

PA シリーズとの接続は Aggregate Ethernet インタフェースを通じておこないます。これはいわゆるスタティックのリンクアグリゲーションと同等の機能のため、AX スイッチ側ではスタティックのリンクアグリゲーションを構成して接続します。

3.2.3 ファイアウォール(PAシリーズ)設定時のポイント

同様に、PA シリーズの設定におけるポイントを以下に示します。

(1) コンフィグ他、各種機能等の設定作業はアクティブ装置のみに対しておこなえば良い。 PA Serise

以下(4)でも述べますが、HA を構成する装置間の設定内容は同期させることが可能です。従って HA を構成するシステムでは各種設定の変更作業および commit はアクティブ側の装置に対してのみおこなえば良いです。

(2) HA構成とする場合、最低限HA1 は冗長接続を推奨。 PA Serise

PA シリーズにて HA 構成を組む場合、2 台の装置間にて Control-Link(HA1)および Data-Link(HA2)(アクティブ-アクティブ構成の場合 HA3 も)というインタフェースの接続が必要です。可能であれば HA1,HA2,HA3 各リンクとも冗長接続とすることが最も望ましいですが、空きポートに余裕が無い場合など、HA 用ポートが十分に用意できない場合は最低限 HA1 だけでも冗長に接続することを推奨します。

Contorl-Link である HA1 は装置間で優先度を決める(アクティブ-パッシブ構成の場合アクティブ側を決める)情報をやりとりしており、HA1 がリンクダウンするといわゆるダブルアクト状態に陥ります。

なお HA1、HA2 については上位機種(PA-4000 シリーズ、PA-5000 シリーズ)の場合、専用のポートがありますが、一般の Ethernet ポートも HA インタフェースとして HA1～HA3 用に割り当てることができるため、HA 用に冗長接続をおこなう場合は一般の Ethernet インタフェースを HA インタフェースに適宜割り当てて冗長経路を追加します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(3) HAでアクティブとする予定の装置は、プライオリティ設定値をデフォルトより小さい値とする。 PA Serise

2 台以上の装置でアクティブ/パッシブ高可用性(HA)構成とする場合、アクティブ/パッシブとなる装置の優先付けとしてプライオリティを設定します。プライオリティは設定値の小さい方が優先されます。

アクティブ/パッシブでの HA 構成をイネーブルとした装置間で Control-Link(HA1)が確立すると、プライオリティ設定値の小さい側の装置がアクティブとなります。このため、アクティブとしたい装置のプライオリティはデフォルトの値(=100)より小さく設定することを推奨します。

(4) HA構成を確認したらコンフィグを同期させること。 PA Serise

HA を構成する場合、ネットワークの論理的に矛盾のないようコンフィグ等の設定も HA 構成の装置間で一致させておく必要がありますが、PA シリーズでは HA 構成の装置間にてコンフィグを同期させる機能があります。
ただしそのコンフィグ同期は自動的にはおこなわれませんので、コンフィグを同期させる際はアクティブ側装置(コンフィグ同期元装置)での GUI 上のコンフィグ同期指示(Dashboard タブ-High-Aveilability ウィジェット中の「sync to peer」 

をクリック)もしくは CLI での同期コマンド実行、あるいは commit 実行をおこなってください。

(5) AXと接続するポート(物理インタフェース)はAggregate Ethernetインタフェースとする。 PA Serise

PA シリーズの上位機種では、回線インタフェースに Aggregate Ethernet インタフェースと呼ぶスタティックリンクアグリゲーション相当の機能があります。AX シリーズスイッチへの接続は、この Aggregate Ethernet インタフェースによりおこなう設定とします。

(6) ネットワーク設定ではゾーンや所属VSYS、仮想ルータ等の設定も忘れずに。 PA Serise

PA シリーズでのネットワークに関する設定では、Ethernet インタフェースや、VLAN を使用する場合の VLAN の設定などの他に、ファイアウォールのポリシー設定等で使用するゾーンの設定が必要です。さらに VSYS を使う場合は所属する VSYS、また Layer3 のインタフェースでは対応させる仮想ルータの設定などが必要となります。これらが設定されていない場合、正しく通信をおこなうことができません。

なお、GUI におけるゾーンや VSYS、仮想ルータ等の設定は Ethernet インタフェースや VLAN の設定画面からも設定のウインドウを呼び出せるようになっています。

(7) PAシリーズはデフォルトではpingに応答しないため注意。 PA Serise

システム構築の際、ネットワークの到達性確認のため ping を使って疎通確認をおこないたいケースもあるかと思いますが、PA シリーズの Layer3 インタフェース(IP アドレスを持つ Ethernet ポートや VLAN)を ping の宛先とした場合、ネットワークに到達性があってもそのままでは ping に応答しません。
PA シリーズのインタフェースにて ping 応答をさせたい場合は、ping 応答を許可する Layer3 インタフェースに対し、あらかじめ Management Profile にて ping を許可する設定としたプロファイルを適用する必要があります。

同様に、管理ポート以外で telnet や Web-GUI(http/https)による装置の管理をおこなう場合も、同様に Management Profile にて管理用のプロファイルを用意し、インタフェースに適用する必要があります。

(8) 必要に応じて各ネットワーク毎の管理ユーザを設定する。 PA Serise

デフォルトで用意されている管理ユーザ(admin)では、各 VSYS の設定はもちろん、ライセンス管理やシグネチャのアップデートなど、PA シリーズ装置全体の管理をおこなうことができますが、新規に管理ユーザを設定する際には、単一または特定の VSYS など、管理できる範囲を設定することができます。
ですので、管理単位の独立した仮想ネットワークにて VSYS を使用する際には、各ネットワークで独立した管理者を割り当てられるよう、各ネットワーク(各 VSYS)向けの管理ユーザを設定することを推奨します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(9) 設定の最後には必ず「Commit」をおこなうこと。

PA Serise

PA シリーズの設定では、各設定で[OK]を選択して設定を終了しても、実行中のコンフィグ(Running Configuration)へはリアルタイムには反映されません。GUI による設定でも CLI による設定でも最終的に入力した設定を装置に反映させる(Candidate Configuration を Running Configuration へ反映させる))ためには Commit コマンドの実行が必要です。

また、HA を構成している場合、アクティブ装置での Commit 実行が正しくおこなわれると、そのままパッシブ装置へのコンフィグ同期もおこなわれます。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

3.2.4 コンフィグレーション例

本構成のコンフィグレーションの例を下記に示します。

(1) コアスイッチ（AX3650S 2 台スタック)の設定

◆ スタンドアロン ⇒ スタック 移行までの設定 <構築ポイント3.2.2-(1)>

メンバスイッチ A (switch 1)《マスタスイッチ(候補)》の設定	
スタックの有効化	
(config)# stack enable After this command execute, please save configuration editing now in startup-config, and please reboot a device. Do you wish to continue ? (y/n): y	スタック機能を有効に設定します。 コンフィグレーションの変更確認と装置の再起動を促すメッセージが表示されますので、「y」を入力します。
(config)# save (config)# exit # reload	コンフィグレーションを保存して、コンフィグレーションコマンドモードから装置管理者モードに戻ります。 装置を手動で再起動します。
スタックの設定	
(config)# interface range tengigabitethernet 1/0/29-30 (config-if-range)# switchport mode stack (config-if-range)# exit	自身のメンバスイッチ A(スイッチ番号 1)のイーサネットインタフェースにスタックポートを設定します。
(config)# switch 1 priority 20	自身のメンバスイッチ A(スイッチ番号 1)のマスタ選出優先度を 20 に設定します。
(config)# switch 2 provision 3650-24t6xw	メンバスイッチ B の装置モデルを設定します。
(config)# interface range tengigabitethernet 2/0/29-30 (config-if-range)# switchport mode stack (config-if-range)# exit	メンバスイッチ B(スイッチ番号 2)のイーサネットインタフェースにスタックポートを設定します。
(config)# switch 2 priority 10	メンバスイッチ B(スイッチ番号 2)のマスタ選出優先度を 10 に設定します。
(config)# save (config)# exit	コンフィグレーションを保存して、コンフィグレーションコマンドモードから装置管理者モードに戻ります。

メンバスイッチ B (switch 2)《バックアップスイッチ(候補)》の設定	
スイッチ番号の設定	
# set switch 2 The switch number was changed to 2. When device restart, the change in the switch number is reflected.	スイッチ番号を「2」に設定します。 スイッチ番号は、装置を再起動した際に反映されます。 本コマンドは運用コマンドです。装置管理者モードで実行してください。
スタックの有効化	
(config)# stack enable After this command execute, please save configuration editing now in startup-config, and please reboot a device. Do you wish to continue ? (y/n): y	スタック機能を有効に設定します。 コンフィグレーションの変更確認と装置の再起動を促すメッセージが表示されますので、「y」を入力します。
(config)# save (config)# exit # reload	コンフィグレーションを保存して、コンフィグレーションコマンドモードから装置管理者モードに戻ります。 装置を手動で再起動します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

メンバスイッチ B (switch 2) 《バックアップスイッチ (候補) 》 の設定	
スタックの設定	
(config)# interface range tengigabitethernet 2/0/29-30 (config-if-range)# switchport mode stack (config-if-range)# exit	自身のメンバスイッチ B(スイッチ番号 2)のイーサネットインタフェースにスタックポートを設定します。
スタックの設定	
(config)# switch 2 priority 1	メンバスイッチ B(スイッチ番号 2)のマスタ選出優先度を 1 に設定します。
(config)# save (config)# exit	コンフィグレーションを保存して、コンフィグレーションコマンドモードから装置管理者モードに戻ります。

以上で、スタック移行の設定は完了です。
次に、メンバスイッチ A とメンバスイッチ B のスタックポートを接続してください。メンバスイッチ B が自動で再起動して 2 台のスタック構成が構築されます。

◆ スタック設定(スタック構成済み)後の設定

C1 (AX3650S-24T6XW) の設定	
VRF の設定	
(config)# vrf definition 10 (config)# vrf definition 20 (config)# vrf definition 30	VRF10,20,30 を使用することを設定します。 **<構築ポイント3.2.2-(2)>**
VLAN の設定	
(config)# vlan 2,10,20,30-32,100-101,200-201,1000	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.1 255.255.0.0 (config-if)# exit	VLAN2 はシステム管理用に VRF を設定せず使用します。 VLAN2 に装置の IP アドレスを設定します。
(config)# interface vlan 10 (config-if)# vrf forwarding 10 (config-if)# ip address 10.0.0.1 255.255.255.0 (config-if)# exit	VLAN10 はVRF10 で使用します。**<構築ポイント3.2.2-(3)>** VLAN10 に IP アドレスを設定します。
(config)# interface vlan 20 (config-if)# vrf forwarding 20 (config-if)# ip address 20.0.0.1 255.255.255.0 (config-if)# exit	VLAN20 はVRF20 で使用します。**<構築ポイント3.2.2-(3)>** VLAN20 に IP アドレスを設定します。
(config)# interface vlan 30 (config-if)# vrf forwarding 30 (config-if)# ip address 30.0.0.1 255.255.255.0 (config-if)# exit	VLAN30 はVRF30 で使用します。**<構築ポイント3.2.2-(3)>** VLAN30 に IP アドレスを設定します。
(config)# interface vlan 31 (config-if)# vrf forwarding 30 (config-if)# ip address 31.0.0.1 255.255.255.0 (config-if)# exit	VLAN31 はVRF30 で使用します。**<構築ポイント3.2.2-(3)>** VLAN31 に IP アドレスを設定します。
(config)# interface vlan 32 (config-if)# vrf forwarding 30 (config-if)# ip address 32.0.0.1 255.255.255.0 (config-if)# exit	VLAN32 はVRF30 で使用します。**<構築ポイント3.2.2-(3)>** VLAN32 に IP アドレスを設定します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

C1（AX3650S-24T6XW）の設定

```
(config)# interface vlan 100
(config-if)# vrf forwarding 10
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# exit

(config)# interface vlan 101
(config-if)# vrf forwarding 10
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# exit

(config)# interface vlan 200
(config-if)# vrf forwarding 20
(config-if)# ip address 192.169.0.1 255.255.255.0
(config-if)# exit

(config)# interface vlan 201
(config-if)# vrf forwarding 20
(config-if)# ip address 192.169.1.1 255.255.255.0
(config-if)# exit

(config)# interface vlan 1000
(config-if)# vrf forwarding 30
(config-if)# exit
```

VLAN100 はVRF10 で使用します。<構築ポイント3.2.2-(3)>
VLAN100 に IP アドレスを設定します。

VLAN101 はVRF10 で使用します。<構築ポイント3.2.2-(3)>
VLAN101 に IP アドレスを設定します。

VLAN200 はVRF20 で使用します。<構築ポイント3.2.2-(3)>
VLAN200 に IP アドレスを設定します。

VLAN201 はVRF20 で使用します。<構築ポイント3.2.2-(3)>
VLAN201 に IP アドレスを設定します。

VLAN1000 は VRF30 で使用しますが、IP アドレスは設定しません。

物理ポートインタフェースの設定

ポートの設定

```
(config)# interface range gigabitethernet 1/0/1,
gigabitethernet 2/0/1
(config-if-range)# link debounce time 0
(config-if-range)# channel-group 11 mode on

(config)# interface range gigabitethernet 1/0/2,
gigabitethernet 2/0/2
(config-if-range)# link debounce time 0
(config-if-range)# channel-group 12 mode on

(config)# interface range tengigabitethernet 1/0/25,
tengigabitethernet 2/0/25
(config-if-range)# link debounce time 0
(config-if-range)# channel-group 10 mode on

(config)# interface range tengigabitethernet 1/0/27,
tengigabitethernet 2/0/27
(config-if-range)# link debounce time 0
(config-if-range)# channel-group 1 mode on

(config)# interface range tengigabitethernet 1/0/28,
tengigabitethernet 2/0/28
(config-if-range)# link debounce time 0
(config-if-range)# channel-group 2 mode on
```

ポート 1/0/1 とポート 2/0/1 は装置 A1 接続用にチャネルグループ 11 を構成します。

ポート 1/0/2 とポート 2/0/2 は装置 A2 接続用にチャネルグループ 12 を構成します。

ポート 1/0/25 とポート 2/0/25 は装置 S1 接続用にチャネルグループ 10 を構成します。

ポート 1/0/27 とポート 2/0/27 はFW1 接続用にチャネルグループ 1 を構成します。<構築ポイント3.2.2-(4)>

ポート 1/0/28 とポート 2/0/28 はFW2 接続用にチャネルグループ 1 を構成します。<構築ポイント3.2.2-(4)>

ポートチャネルの設定

```
(config)# interface range port-channel 1-2
(config-if-range)# switchport mode trunk
(config-if-range)# switchport trunk allowed vlan
2,10,20,30-32,1000

(config)# interface port-channel 10
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan
2,10,20,30,1000

(config)# interface port-channel 11
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 2,100-101

(config)# interface port-channel 12
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 2,200-201
```

ポートチャネル 1 と 2 はトランクポートとし VLAN2,10,20,3-32,1000 の転送を許可します。

ポートチャネル 10 はトランクポートとし VLAN2,10,20,30,1000 の転送を許可します。

ポートチャネル 11 はトランクポートとし VLAN2,100-101 の転送を許可します。

ポートチャネル 12 はトランクポートとし VLAN2,200-201 の転送を許可します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

C1（AX3650S-24T6XW）の設定	
デフォルトルートの設定	
(config)# ip route vrf10 0.0.0.0 0.0.0.0 10.0.0.10 (config)# ip route vrf20 0.0.0.0 0.0.0.0 20.0.0.10 (config)# ip route vrf30 0.0.0.0 0.0.0.0 30.0.0.10	VRF10 でのデフォルトルートを設定します。 VRF20 でのデフォルトルートを設定します。 VRF30 でのデフォルトルートを設定します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

(2) サーバ用アクセススイッチ（AX2530S)の設定

S1（AX2530S-24T4X）の設定	
スパニングツリーの設定	
(config)# spanning-tree disable	AX シリーズではデフォルトで PVST+が有効になっているため、これを抑止します。
VLAN の設定	
(config)# vlan 2,10,20,30,1000	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.0.5 255.255.0.0	VLAN2 はシステム管理用に使用します。 VLAN2 に IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range tengigabitethernet 0/27-28 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on (config)# interface range gigabitethernet 0/1-4 (config-if-range)# switchport access vlan 10 (config)# interface range gigabitethernet 0/5-8 (config-if-range)# switchport access vlan 20 (config)# interface range gigabitethernet 0/9-12 (config-if-range)# switchport access vlan 30 (config)# interface gigabitethernet 0/20 (config-if)# switchport access vlan 1000 (config)# interface gigabitethernet 0/24 (config-if)# switchport access vlan 2	ポート 0/27-28 は装置 C1 接続用にチャネルグループ 1 を構成します。 ポート 0/1-4 は開発部ローカルサーバ接続用に VLAN10 のアクセスポートとして構成します。 ポート 0/5-8 は総務部ローカルサーバ接続用に VLAN20 のアクセスポートとして構成します。 ポート 0/9-12 は外部公開サーバ接続用に VLAN30 のアクセスポートとして構成します。 ポート 0/20 は外部接続用に VLAN1000 のアクセスポートとして構成します。 ポート 0/24 はシステム管理 PC 接続用に VLAN2 のアクセスポートとして構成します。
ポートチャネルの設定	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20,30,1000	ポートチャネル 1 はトランクポートとし VLAN2,10,20,30,1000 の転送を許可します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

(3) 端末PC用アクセススイッチ（AX1240S)の設定）

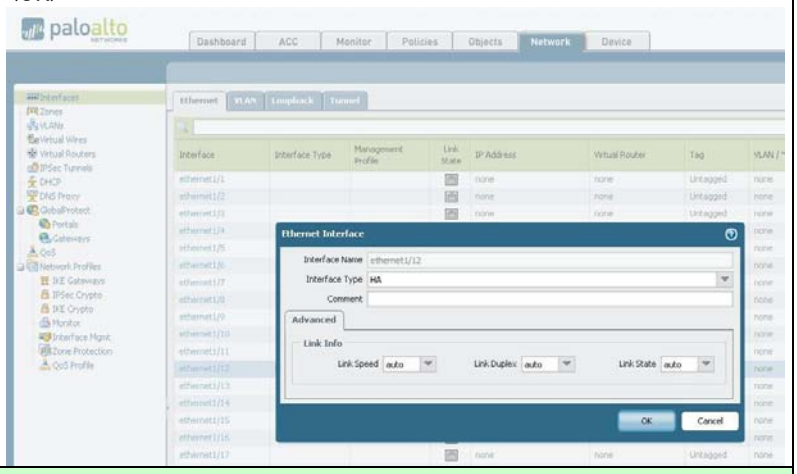
A1（AX1240S-24T2C）の設定	
スパニングツリーの抑止	
(config)# spanning-tree disable	AX シリーズではデフォルトで PVST+が有効となっていますが、FT 構成とする場合はこれを抑止します。
VLAN の設定	
(config)# vlan 2,100-101	使用する VLAN の設定をおこないます。
VLAN インタフェースの設定	
(config)# interface vlan 2 (config-if)# ip address 172.255.1.1 255.255.0.0	VLAN2 をシステム管理用に使用するため、装置の IP アドレスを設定します。
物理ポートインタフェースの設定	
ポートの設定	
(config)# interface range gigabitethernet 0/25-26 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on (config)# interface range fastethernet 0/1-12 (config-if-range)# switchport access vlan 100 (config)# interface fastethernet 0/13-24 (config-if-range)# switchport access vlan 101	ポート 0/25-26 は装置 C1 接続用にチャネルグループ 1 を構成します。 ポート 0/1-12 は会社 A 端末 PC のセグメント 1 接続用に VLAN100 のアクセスポートとして構成します。 ポート 0/13-24 は会社 A 端末 PC のセグメント 2 接続用に VLAN101 のアクセスポートとして構成します。
ポートチャネルの設定	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,100-101	ポートチャネル 1 はトランクポートとし VLAN2,100-101 の転送を許可します。
装置のリモート管理に関する設定	
(config)# logging host 172.255.0.200 (config)# line vty 0 1	syslog 採取用ホストを指定します。 telnet によるログインを許可します。

装置 B1 の設定は使用する VLAN ID と装置アドレスが異なる以外は装置 A1 の設定と同様です。
(VLAN：100-101→200-201、装置アドレス：172.255.1.1→172.255.2.1)

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

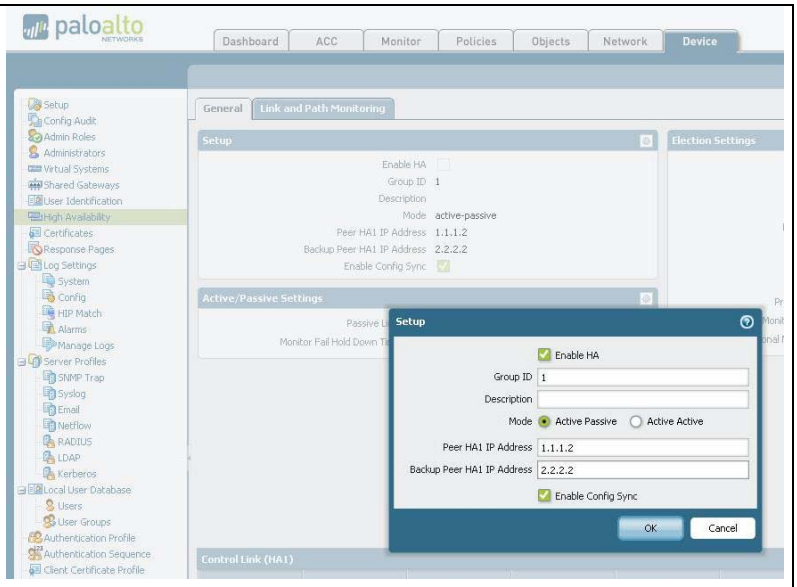
(4) ファイアウォール（PAシリーズ)の設定

PA シリーズで HA 構成を組む場合、アクティブとする装置にて基本設定をおこなっておきます。

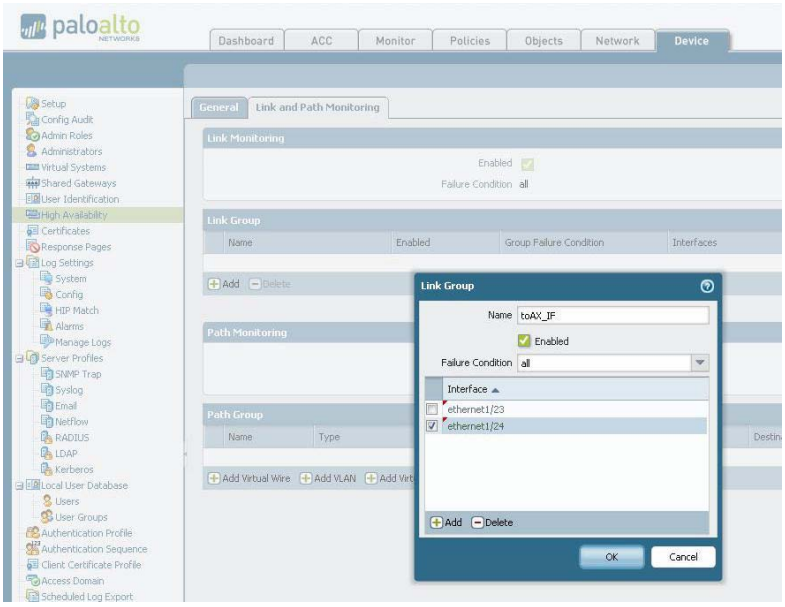
FW1（PA-5060:アクティブ側）の設定 <構築ポイント3.2.3-(1)>	
CLI	**GUI（画面の例は3.1.4(4)を参考ください）**
HA(冗長構成)の設定	
HA1 冗長接続用に Ethernet インタフェースに HA インタフェースを設定	
`# set network interface ethernet ethernet1/12 ha`	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** Interface – ethernet1/12 選択で Ethernet Interface 設定ウインドウ [Interface Type] HA <OK> 
HA を設定	

`# set deviceconfig high-availability enabled yes`
 	
`# set deviceconfig high-availability group 1 mode active-passive`
 	
`# set deviceconfig high-availability group 1 peer-ip 1.1.1.2`
 	
`# set deviceconfig high-availability group 1 peer-ip-backup 2.2.2.2`
 	
`# set deviceconfig high-availability group 1 configration-synchronization enabled yes`
 	
`# set deviceconfig high-availability group 1 election-option device-priority 10`
 	
`# set deviceconfig high-availability interface ha1 port dedicated-ha1 ip-address 1.1.1.1 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha1-backup port ethernet1/12 ip-address 2.2.2.1 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha2 port dedicated-ha2`
	[Device]＞[High Availability]＞[General]タブ画面
	・Setup 設定ウインドウ
	[Enable HA]にチェック
	[Group ID] 1
	[Mode] Active Passive
	[Peer HA1 IP Address] 1.1.1.2
	[Backup Peer HA1 IP Address] 2.2.2.2
	[Enable Config Sync]にチェック
	<OK>
	
	・Election Settings設定ウインドウ **<構築ポイント3.2.3-(3)>**
	[Device Priority] 10
	<OK>
	
	・Control Link(HA1) – Primary 設定ウインドウ
	[Port] dedicated-ha1(Dedicated out of band HA1 interface)
	[IP Address] 1.1.1.1
	[Netmask] 255.255.255.0
	<OK>
	
	・Control Link(HA1) – Backup設定ウインドウ **<構築ポイント3.2.3-(2)>**
	[Port] ethernet1/12
	[IP Address] 2.2.2.1
	[Netmask] 255.255.255.0
	<OK>
	・Data Link(HA2)設定 – Primary 設定ウインドウ
	[Port] dedicated-ha2(Dedicated out of band HA2 interface)
	<OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

<table>
<tr><td></td><td> 
</td></tr>
<tr><td colspan="2">リンクモニタリングの設定</td></tr>
<tr><td><pre>#set deviceconfig high-availability
group 1 monitoring link-monitoring
link-group toAX interface
[ethernet1/23 ethernet1/24]

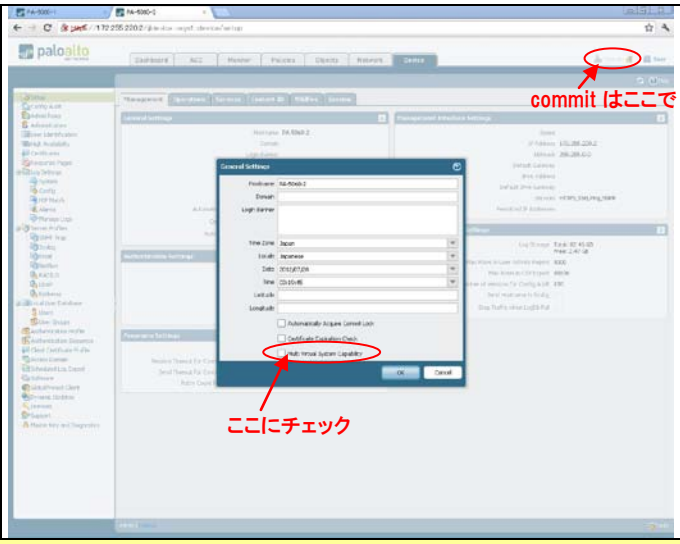
#set deviceconfig high-availability
group 1 monitoring link-monitoring
link-group toAX enabled yes

#set deviceconfig high-availability
group 1 monitoring link-monitoring
link-group toAX failure-condition all</pre></td><td>[Device]＞[High Availability]＞[Link and Path Monitoring]タブ画面
・[Link Group]にて[Add] – Link Group 設定ウインドウ
[Name] toAX
[Enabled]にチェック
[Failure Condition] all
[Interfaces▲] ethernet1/23, ethernet1/24 を Add
〈OK〉
 
</td></tr>
<tr><td colspan="2">バーチャルシステム(VSYS)使用の設定</td></tr>
<tr><td colspan="2">バーチャルシステムの使用を設定し、commitして設定を反映 〈構築ポイント3.2.2-(9)〉</td></tr>
<tr><td>※一旦quitしオペレーショナルモードより設定
<pre>> set system setting multi-vsys on
> configure

commit</pre></td><td>[Device]＞[Setup]＞[Management]タブ画面
・General Settings 設定ウインドウ
[Multi Virtual System Capability]にチェック
〈OK〉

画面右上 Commit をクリック</td></tr>
</table>

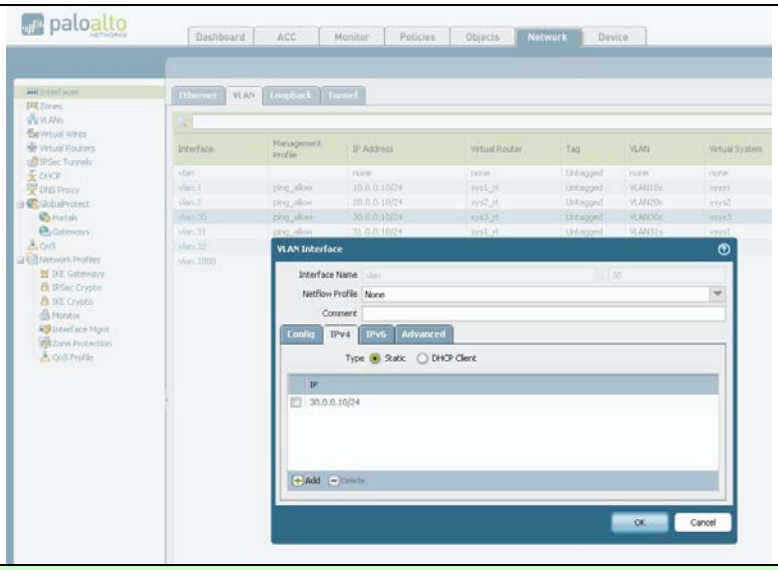
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

	
インタフェースの設定	
Aggregate Ethernetインタフェース作成および設定 <構築ポイント3.2.2-(5)>	
#set network interface aggregate-ethernet ae1 layer2 #set network interface ethernet ethernet1/23 aggregate-group ae1 #set network interface ethernet ethernet1/24 aggregate-group ae1	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** ・[Add Aggregate Group]で AggregateGroup 設定ウインドウ [Interface name] ae 1 <OK> ・Interface – ethernet1/23 選択で Ethernet Interface 設定ウインドウ [Interface name] ae1 [Interface Type] Aggregate Ethernet <OK> ・Interface – ethernet1/24 選択で Ethernet Interface 設定ウインドウ [Interface name] ae1 [Interface Type] Aggregate Ethernet <OK>
タグ付きインタフェース(Layer2 Subinterface)作成および設定	
#set network interface aggregate-ethernet ae1 layer2 units ae1.1 tag 10 #set network interface aggregate-ethernet ae1 layer2 units ae1.2 tag 20 #set network interface aggregate-ethernet ae1 layer2 units ae1.30 tag 30 #set network interface aggregate-ethernet ae1 layer2 units ae1.31 tag 31 #set network interface aggregate-ethernet ae1 layer2 units ae1.32 tag 32 #set network interface aggregate-ethernet ae1 layer2 units ae1.1000 tag 1000 #set network interface aggregate-ethernet ae1 layer2 units ae1.9002 tag 2	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** ・[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　1　*(Interface 名=ae1.1 となる)* [Tag] 10 <OK> ・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　2　*(Interface 名=ae1.2 となる)* [Tag] 20 <OK> ・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　30　*(Interface 名=ae1.30 となる)* [Tag] 30 <OK> ・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　31　*(Interface 名=ae1.31 となる)* [Tag] 31 <OK> ・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　32　*(Interface 名=ae1.32 となる)* [Tag] 32 <OK> ・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　1000　*(Interface 名=ae1.1000 となる)* [Tag] 1000 <OK> ・再度[Add Layer2 Subinterface]で Layer2 Subinterface 設定ウインドウ [Interface name] ae1　9002　*(Interface 名=ae1.9002 となる)* [Tag] 2 <OK>

Copyright © 2013,　ALAXALA Networks Corporation. All rights reserved.

VLAN インタフェースの作成と設定	
#set network interface vlan units vlan.1 ip 10.0.0.10/24	**[Network]＞[Interfaces]＞[VLAN]タブ画面** ・[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 1 *（VLAN Interface 名=vlan.1 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 10.0.0.10/24 <OK>
#set network interface vlan units vlan.2 ip 20.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 2 *（VLAN Interface 名=vlan.2 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 20.0.0.10/24 <OK>
#set network interface vlan units vlan.30 ip 30.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 30 *（VLAN Interface 名=vlan.30 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 30.0.0.10/24 <OK>
#set network interface vlan units vlan.31 ip 31.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 31 *（VLAN Interface 名=vlan.31 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 31.0.0.10/24 <OK>
#set network interface vlan units vlan.32 ip 32.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 32 *（VLAN Interface 名=vlan.32 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 32.0.0.10/24 <OK>
#set network interface vlan units vlan.1000 ip 100.0.0.10/24	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 1000 *（VLAN Interface 名=vlan.1000 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 100.0.0.10/24 <OK>
#set network interface vlan units vlan.9002 ip 172.255.0.10/16	・再度[Add]で VLAN interface 設定ウインドウ Config タブ [Interface Name] vlan 9002 *（VLAN Interface 名=vlan.9002 となる）* IPv4 タブ [Type] Static [Add]で IPv4 アドレス 172.255.0.10/16 <OK>

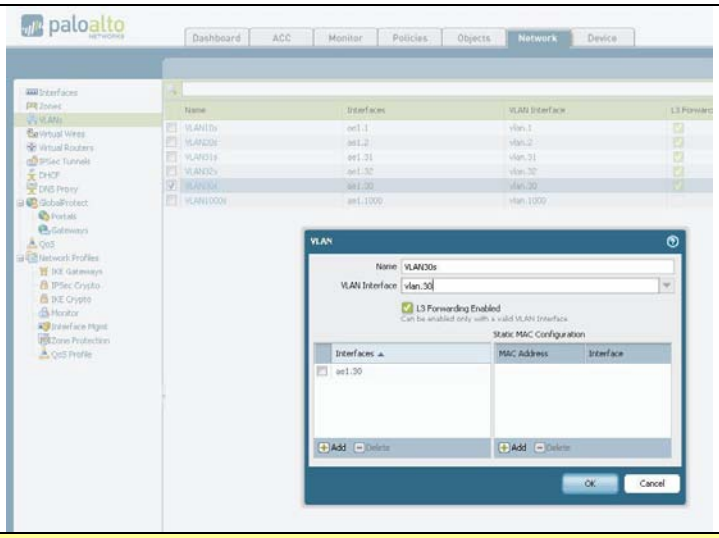
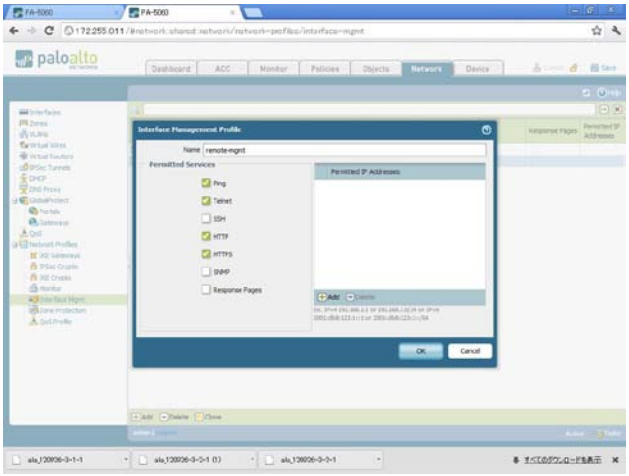
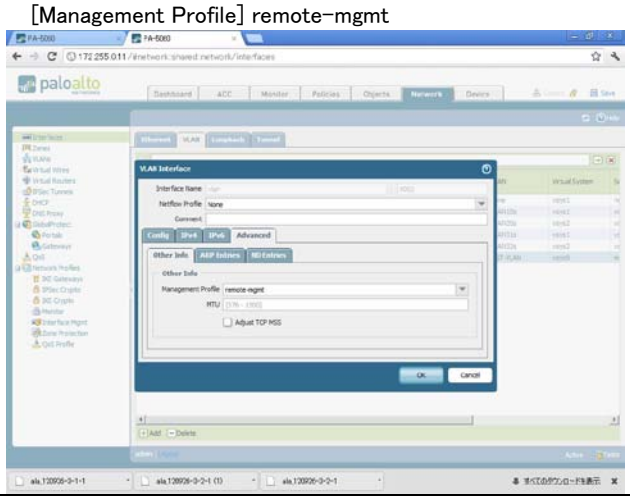
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.



VLAN の作成

`#set network vlan VLAN10s interface ae1.1 virtual-interface interface vlan.1 l3-forwarding yes`	**[Network]＞[VLANs]タブ画面** ・[Add]で VLAN 設定ウインドウ [Name] VLAN10s [VLAN Interface] vlan.1 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.1 を Add <OK>
`#set network vlan VLAN20s interface ae1.2 virtual-interface interface vlan.2 l3-forwarding yes`	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN20s [VLAN Interface] vlan.2 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.2 を Add <OK>
`#set network vlan VLAN30s interface ae1.30 virtual-interface interface vlan.30 l3-forwarding yes`	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN30s [VLAN Interface] vlan.30 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.30 を Add <OK>
`#set network vlan VLAN31s interface ae1.31 virtual-interface interface vlan.31 l3-forwarding yes`	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN31s [VLAN Interface] vlan.31 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.31 を Add <OK>
`#set network vlan VLAN32s interface ae1.32 virtual-interface interface vlan.32 l3-forwarding yes`	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN32s [VLAN Interface] vlan.32 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.32 を Add <OK>
`#set network vlan VLAN1000s interface ae1.1000 virtual-interface interface vlan.1000 l3-forwarding yes`	・再度[Add]で VLAN 設定ウインドウ [Name] VLAN1000s [VLAN Interface] vlan.1000 [L3 Forwarding Enabled]にチェック [Interfaces▲] ae1.1000 を Add <OK>
`#set network vlan MGT-VLAN interface ae1.9002 virtual-interface interface vlan.9002`	・再度[Add]で VLAN 設定ウインドウ [Name] MGT-VLAN [VLAN Interface] vlan.9002 [Interfaces▲] ae1.9002 を Add <OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

<table>
<tr><td></td><td>  </td></tr>
<tr><td colspan="2">Layer3 インタフェース用管理プロファイルの設定 〈構築ポイント3.2.3-(7)〉</td></tr>
<tr><td colspan="2">装置のリモート管理用プロファイルの設定</td></tr>
<tr><td>#set network profiles
interface-management-profile
remote-mgmt ping yes telnet yes http yes
https yes</td><td>[Network]＞[Network Profiles]−[Interface mgmt] 画面
・[Add]で Interface Management Profile 設定ウインドウ
[Name] remote−mgmt
Permitted Services 内の[Ping][Telnet][HTTP][HTTPS]等、
必要な項目にチェック
[Permitted IP Address] 必要に応じて、許可するホストまたは
ネットワークアドレスを追加
〈OK〉
  </td></tr>
<tr><td>#set network interface vlan units
vlan.9002 interface-management-profile
remote-mgmt</td><td>[Network]＞[Interfaces]＞[VLAN]タブ画面
・[Interface]以下 vlan.9002 を選択で VLAN interface 設定ウインドウ
Advanced タブ−OtherInfo タブ
[Management Profile] remote−mgmt
  </td></tr>
</table>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

Layer3 インタフェースを ping 応答可とする設定（必要に応じて）

```
#set network profiles
interface-management-profile
ping_allow ping yes
```

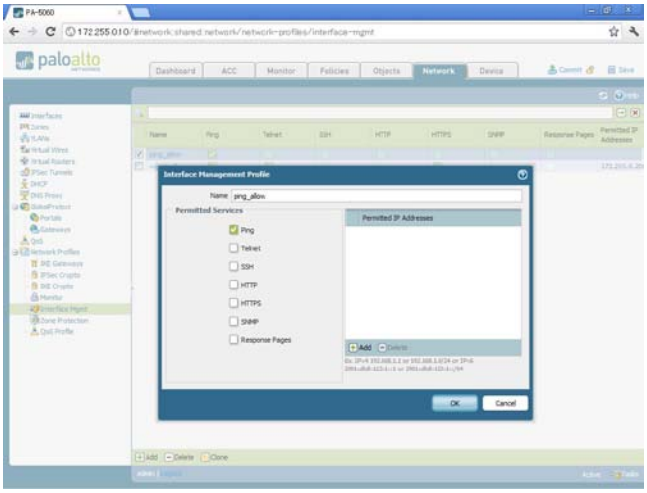
[Network]＞[Network Profiles]-[Interface mgmt] 画面

・[Add]で Interface Management Profile 設定ウインドウ

[Name] ping_allow

Permitted Services 内の[Ping]にチェック

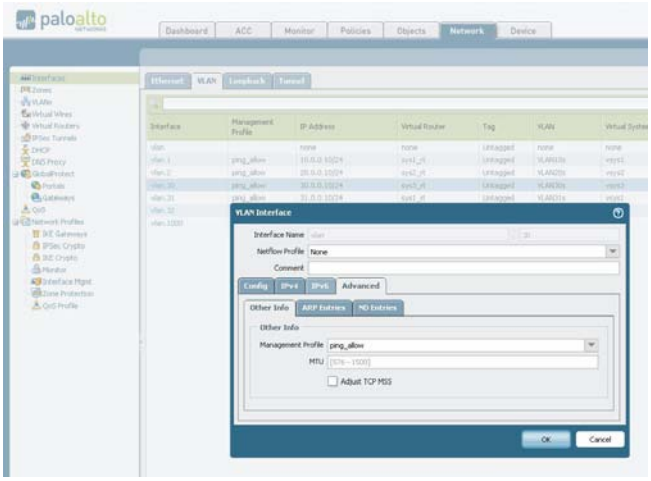
<OK>



この設定以降、Layer3 としたインタフェースの[Advanced]-[Other Info]タブ以下で[Management Profile]で ping_allow が選択できるようになるため、ping 応答させたい Layer3 インタフェースで適宜選択する。

(vlan.30への設定例)

```
#set network interface vlan units
vlan.30 interface-management-profile
ping_allow
```



VSYS1（開発部システム用ファイアウォール）の設定

VSYS を作成

```
#delete vsys vsys1 import network
interface ethernet1/12

#set vsys vsys1 import network
interface [ ae1.1 ae1.31 vlan.1
vlan.31 ]
```

[Device]＞[Virtual Systems] 画面

・[Add]で vsys 設定ウインドウ

[ID] 1

General タブ － [Interfaces▲] ae1.1, ae1.31, vlan.1, vlan.31 を add

<OK>

仮想ルータを設定 <構築ポイント3.2.3-(6)>

```
#set network virtual-router sys1_rt
interface [ vlan.1 vlan.31 ]
routing-table ip static-route default
destination 0.0.0.0/0 nexthop
ip-address 31.0.0.254
```

[Network]＞[Virtual Routers] 画面

・[Add]で Virtual Router 設定ウインドウ

General タブ

[Name] sys1_rt

[Interfaces▲] vlan.1, vlan.31 を Add

Static Routes タブ － IPv4 タブ

[Add]で Virtual Router － Static Route － IPv4 設定ウインドウ

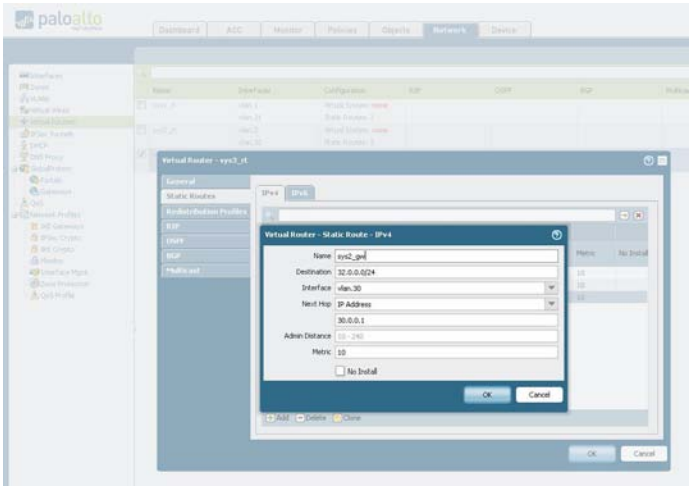
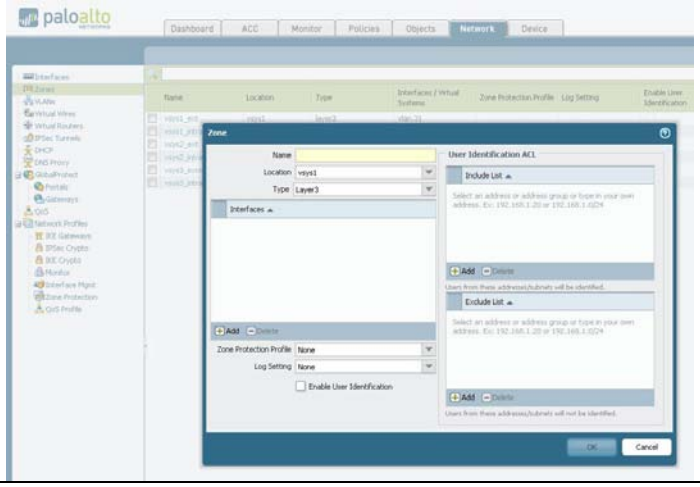
[Name] default

[Destination] 0.0.0.0/0

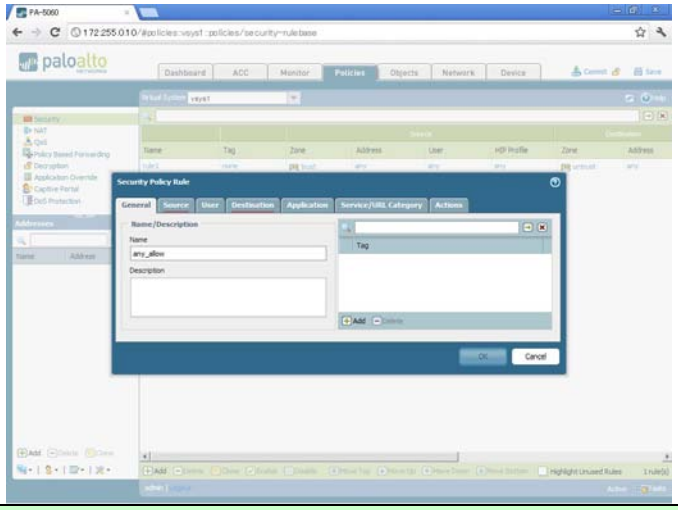
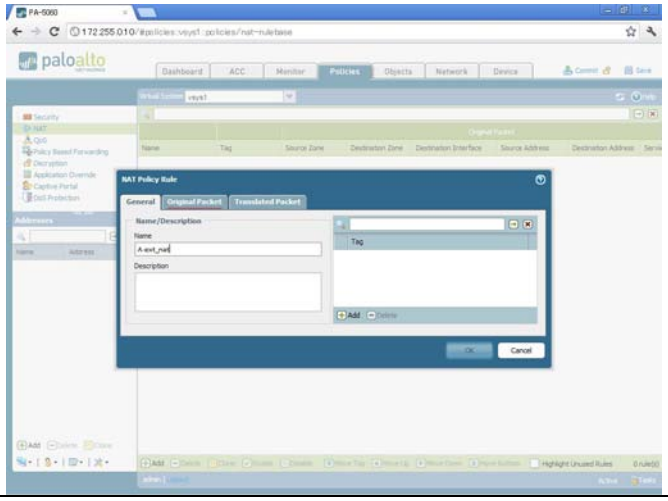
[Next Hop] IP Address を選択し、下の行に 31.0.0.254 入力

<OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

#set network virtual-router sys1_rt routing-table ip static-route A-TERM1 destination 192.168.0.0/24 nexthop ip-address 10.0.0.1	再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] A-TERM1 [Destination] 192.168.0.0/24 [Next Hop] IP Address を選択し、下の行に 10.0.0.1 入力 <OK>
#set network virtual-router sys1_rt routing-table ip static-route A-TERM2 destination 192.168.1.0/24 nexthop ip-address 10.0.0.1	再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] A-TERM2 [Destination] 192.168.1.0/24 [Next Hop] IP Address を選択し、下の行に 10.0.0.1 入力 <OK>
	<OK> 
#set vsys vsys1 import network virtual-router sys1_rt	**[Device]＞[Virtual Systems] 画面** ・vsys1 を選択 General タブ – [Virtual Routers▲] sys1_rt を add <OK>
ゾーンを設定 <構築ポイント3.2.3-(6)>	
#set vsys vsys1 zone vsys1_trust network layer3 vlan.1	**[Network]＞[Zones] 画面** ・[Add]で Zone 設定ウインドウ [Name] vsys1_trust [Location] vsys1 [Type] Layer3 [Interfaces▲] vlan.1 を add <OK>
#set vsys vsys1 zone vsys1_untrust network layer3 vlan.31	・再度[Add]で Zone 設定ウインドウ [Name] vsys1_untrust [Location] vsys1 [Type] Layer3 [Interfaces▲] vlan.31 を add <OK> 

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

セキュリティ(フィルタ)を設定	
#set vsys vsys1 rulebase security rules any_allow from any to any #set vsys vsys1 rulebase security rules any_allow source any destination any #set vsys vsys1 rulebase security rules any_allow application any service any action allow	**[Policies]＞[Security] 画面** – [Virtual System] vsys1 選択 ・[Add]で Security Policy Rule 設定ウインドウ General タブ [Name] any_allow Source タブ Source Zone および Source Address の上の[Any]にチェック Destination タブ Destination Zone の上[Any]選択 Destination Address の上[Any]にチェック Actions タブ Action Setting [Action] allow <OK> 
NAT ポリシーの追加	
#set vsys vsys1 rulebase nat rules A-ext_nat to vsys1_untrust from vsys1_trust #set vsys vsys1 rulebase nat rules A-ext_nat source any destination any service any #set vsys vsys1 rulebase nat rules A-ext_nat source-translation dynamic-ip-and-port interface-address interface vlan.31	**[Policies]＞[NAT] 画面** – [Virtual System] vsys1 選択 ・[Add]で NAT Policy Rule 設定ウインドウ General タブ [Name] A-ext_nat Original Packet タブ [Source Zone] vsys1_trust を Add [Destination Zone] vsys1_untrust [Service] Any [Source Address] Any にチェック [Destination Address] Any にチェック Translated Packet タブ [Translation Type] Dynamic IP and Port [Address Type] Interface Address [Interface] vlan.31 [IP Adress] 31.0.0.10/24 <OK> 

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

VSYS2（総務部システム用ファイアウォール）の設定	
VSYS を作成	
`#set vsys vsys2 import network interface [ ae1.2 ae1.32 vlan.2 vlan.32 ]`	**[Device]＞[Virtual Systems] 画面** ・[Add]で vsys 設定ウインドウ [ID] 2 General タブ – [Interfaces▲] ae1.2, ae1.32, vlan.2, vlan.32 を add <OK>
仮想ルータを設定 <構築ポイント3.2.3-(6)>	

`#set network virtual-router sys2_rt interface [ vlan.2 vlan.32 ]`
`routing-table ip static-route default destination 0.0.0.0/0 nexthop ip-address 32.0.0.254`
 	
`#set network virtual-router sys2_rt routing-table ip static-route B-TERM1 destination 192.169.0.0/24 nexthop ip-address 20.0.0.1`
 	
`#set network virtual-router sys2_rt routing-table ip static-route B-TERM2 destination 192.169.1.0/24 nexthop ip-address 20.0.0.1`
 	
`#set vsys vsys2 import network virtual-router sys2_rt`
	[Network]＞[Virtual Routers] 画面
	・[Add]で Virtual Router 設定ウインドウ
	General タブ
	[Name] sys2_rt
	[Interfaces▲] vlan.2 vlan.32 を Add
	Static Routes タブ – IPv4 タブ
	[Add]で Virtual Router – Static Route – IPv4 設定ウインドウ
	[Name] default
	[Destination] 0.0.0.0/0
	[Next Hop] IP Address を選択し、下の行に 32.0.0.254 入力
	<OK>
	再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ
	[Name] B-TERM1
	[Destination] 192.169.0.0/24
	[Next Hop] IP Address を選択し、下の行に 20.0.0.1 入力
	<OK>
	再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ
	[Name] B-TERM2
	[Destination] 192.1691.0/24
	[Next Hop] IP Address を選択し、下の行に 20.0.0.1 入力
	<OK>
	<OK>
	[Device]＞[Virtual Systems] 画面
	・vsys1 を選択
	General タブ – [Virtual Routers▲] sys2rt を add
	<OK>

ゾーンを設定 <構築ポイント3.2.3-(6)>	

`#set vsys vsys2 zone vsys2_trust network layer3 vlan.2`
 	
`#set vsys vsys2 zone vsys2_untrust network layer3 vlan.32`
	[Network]＞[Zones] 画面
	・[Add]で Zone 設定ウインドウ
	[Name] vsys2_trust
	[Location] vsys2
	[Type] Layer3
	[Interfaces▲] vlan.2 を add
	<OK>
	・再度[Add]で Zone 設定ウインドウ
	[Name] vsys2_untrust
	[Location] vsys2
	[Type] Layer3
	[Interfaces▲] vlan.32 を add
	<OK>

セキュリティ(フィルタ)を設定	

`#set vsys vsys2 rulebase security rules any_allow from any to any`
 	
`#set vsys vsys2 rulebase security rules any_allow source any destination any`
 	
`#set vsys vsys2 rulebase security rules any_allow application any service any action allow`
	[Policies]＞[Security] 画面 – [Virtual System] vsys2 選択
	・[Add]で Security Policy Rule 設定ウインドウ
	General タブ
	[Name] any_allow
	Source タブ
	Source Zone および Source Address の上の[Any]にチェック
	Destination タブ
	Destination Zone の上[Any]選択
	Destination Address の上[Any]にチェック
	Actions タブ
	Action Setting [Action] allow
	<OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

NAT ポリシーの追加	
#set vsys vsys2 rulebase nat rules B-ext_nat to vsys2_untrust from vsys2_trust #set vsys vsys2 rulebase nat rules B-ext_nat source any destination any service any #set vsys vsys2 rulebase nat rules B-ext_nat source-translation dynamic-ip-and-port interface-address interface vlan.32	**[Policies]＞[NAT] 画面** – [Virtual System] vsys2 選択 ・[Add]で NAT Policy Rule 設定ウインドウ General タブ [Name] B-ext_nat Original Packet タブ [Source Zone] vsys2_trust を Add [Destination Zone] vsys2_untrust [Service] Any [Source Address] Any にチェック [Destination Address] Any にチェック Translated Packet タブ [Translation Type] Dynamic IP and Port [Address Type] Interface Address [Interface] vlan.32 [IP Adress] 32.0.0.10/24 <OK>
VSYS3 (外部接続とのファイアウォール)の設定	
VSYS を作成	
#set vsys vsys3 import network interface [ae1.30 ae1.1000 vlan.30 vlan.1000]	**[Device]＞[Virtual Systems] 画面** ・[Add]で vsys 設定ウインドウ [ID] 3 General タブ – [Interfaces▲] ae1.30, ae1.1000, vlan.30, vlan.1000 を add <OK>
仮想ルータを設定 <構築ポイント3.2.3-(6)>	
#set network virtual-router sys3_rt interface [vlan.30 vlan.1000] routing-table ip static-route default destination 0.0.0.0/0 nexthop ip-address 100.0.0.254 #set network virtual-router sys3_rt routing-table ip static-route A-INTRA destination 31.0.0.0/24 nexthop ip-address 30.0.0.1 #set network virtual-router sys3_rt routing-table ip static-route B-INTRA destination 32.0.0.0/24 nexthop ip-address 30.0.0.1 #set vsys vsys3 import network virtual-router sys3_rt	**[Network]＞[Virtual Routers] 画面** ・[Add]で Virtual Router 設定ウインドウ General タブ [Name] sys2_rt [Interfaces▲] vlan.30 vlan.1000 を Add Static Routes タブ – IPv4 タブ [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] default [Destination] 0.0.0.0/0 [Next Hop] IP Address を選択し、下の行に 100.0.0.254 入力 <OK> 再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] A-INTRA [Destination] 31.0.0.0/24 [Next Hop] IP Address を選択し、下の行に 30.0.0.1 入力 <OK> 再度 [Add]で Virtual Router – Static Route – IPv4 設定ウインドウ [Name] B-INTRA [Destination] 32.0.0.0/24 [Next Hop] IP Address を選択し、下の行に 30.0.0.1 入力 <OK> <OK> **[Device]＞[Virtual Systems] 画面** ・vsys1 を選択 General タブ – [Virtual Routers▲] sys3_rt を add <OK>
ゾーンを設定 <構築ポイント3.2.3-(6)>	
#set vsys vsys3 zone vsys3_trust network layer3 vlan.30	**[Network]＞[Zones] 画面** ・[Add]で Zone 設定ウインドウ [Name] vsys3_trust [Location] vsys3 [Type] Layer3 [Interfaces▲] vlan.30 を add <OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

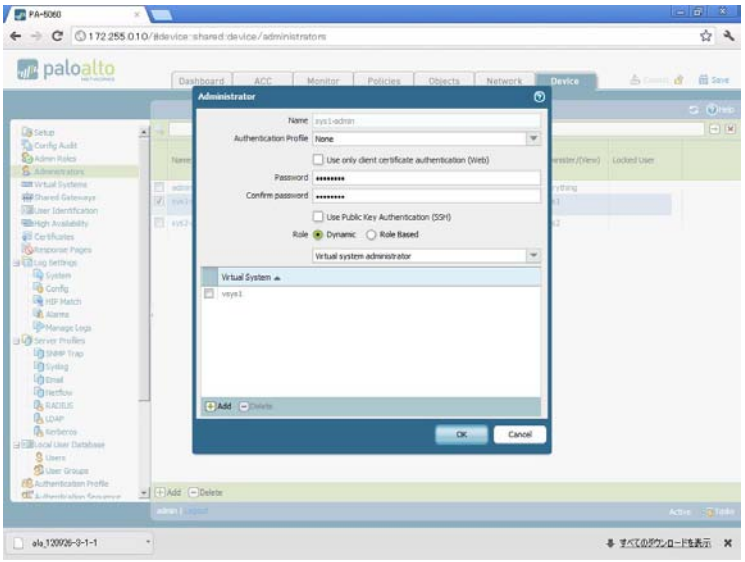
#set vsys vsys3 zone vsys3_untrust network layer3 vlan.1000	・再度[Add]で Zone 設定ウインドウ [Name] vsys3_untrust [Location] vsys3 [Type] Layer3 [Interfaces▲] vlan.1000 を add <OK>
セキュリティ(フィルタ)を設定	
#set vsys vsys3 rulebase security rules any_allow from any to any #set vsys vsys3 rulebase security rules any_allow source any destination any #set vsys vsys3 rulebase security rules any_allow application any service any action allow	**[Policies]＞[Security] 画面** – [Virtual System] vsys3 選択 ・[Add]で Security Policy Rule 設定ウインドウ General タブ [Name] any_allow Source タブ Source Zone および Source Address の上の[Any]にチェック Destination タブ Destination Zone の上[Any]選択 Destination Address の上[Any]にチェック Actions タブ Action Setting [Action] allow <OK>
NAT ポリシーの追加	
#set vsys vsys3 rulebase nat rules Ext_nat to vsys3_untrust from vsys3_trust #set vsys vsys3 rulebase nat rules B-ext_nat source any destination any service any #set vsys vsys3 rulebase nat rules Ext_nat source-translation dynamic-ip-and-port interface-address interface vlan.1000	**[Policies]＞[NAT] 画面** – [Virtual System] vsys3 選択 ・[Add]で NAT Policy Rule 設定ウインドウ General タブ [Name] Ext_nat Original Packet タブ [Source Zone] vsys3_trust を Add [Destination Zone] vsys3_untrust [Service] Any [Source Address] Any にチェック [Destination Address] Any にチェック Translated Packet タブ [Translation Type] Dynamic IP and Port [Address Type] Interface Address [Interface] vlan.1000 [IP Adress] 100.0.0.10/24 <OK>
VSYS9 (システム管理用 VSYS)の設定	
VSYS を作成	
#set vsys vsys9 import network interface [ae1.9002 vlan.9002]	**[Device]＞[Virtual Systems] 画面** ・[Add]で vsys 設定ウインドウ [ID] 9 General タブ – [Interfaces▲] ae1.9002, vlan.9002 を add <OK>
仮想ルータを設定 <構築ポイント3.1.3-(6)>	
#set network virtual-router sys2_rt interface [vlan.9002] #set vsys vsys9 import network virtual-router mgt_rt	**[Network]＞[Virtual Routers] 画面** ・[Add]で Virtual Router 設定ウインドウ General タブ [Name] mgt_rt [Interfaces▲] vlan.9002 を Add <OK> **[Device]＞[Virtual Systems] 画面** ・vsys9 を選択 General タブ – [Virtual Routers▲] mgt_rt を add <OK>

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

ゾーンを設定 <構築ポイント3.1.3-(6)>	
`#set vsys vsys9 zone mgt-zone network layer3 vlan.9002`	**[Network]＞[Zones] 画面** ・[Add]で Zone 設定ウインドウ [Name] mgt-zone [Location] vsys9 [Type] Layer3 [Interfaces▲] vlan.9002 を add <OK>
セキュリティ(フィルタ)を設定	

`#set vsys vsys9 rulebase security rules any_allow from any to any`
 	
`#set vsys vsys9 rulebase security rules any_allow source any destination any`
 	
`#set vsys vsys9 rulebase security rules any_allow application any service any action allow`
	[Policies]＞[Security] 画面 – [Virtual System] vsys9 選択
	・[Add]で Security Policy Rule 設定ウインドウ
	General タブ
	[Name] any_allow
	Source タブ
	Source Zone および Source Address の上の[Any]にチェック
	Destination タブ
	Destination Zone の上[Any]選択
	Destination Address の上[Any]にチェック
	Actions タブ
	Action Setting [Action] allow
	<OK>

VSYS管理ユーザの追加（必要に応じて）<構築ポイント3.2.3-(8)>	
VSYS1 管理ユーザの追加	

`#set mgt-config users sys1-admin permissions role-based vsysadmin localhost.localdomain vsys vsys1`
 	
`#set mgt-config users sys1-admin password`
`Enter password : sys1-admin用パスワード`
`Confirm password : もう一度パスワード入力`
	[Device]＞[Administrators] 画面
	・[Add]で Administrator 設定ウインドウ
	[Name] sys1-admin
	[Password] *sys1-admin 用パスワード*
	[Confirm password] *もう一度パスワード入力*
	[Virtual system administrator]を選択
	[Virtual System] vsys1 を Add
	<OK>
	 

設定内容の反映 <構築ポイント3.2.3-(9)>	
`# commit`	画面右上 Commit をクリック

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

続いて、パッシブとして使用する装置の設定をマスタ装置と接続する前に以下のように設定します。

FW2 (PA-5060:パッシブ側) の設定	
CLI	**GUI**
HA の設定	
HA1 冗長接続用に Ethernet インタフェースに HA インタフェースを設定	
`# set network interface ethernet ethernet1/12 ha`	**[Network]＞[Interfaces]＞[Ethernet]タブ画面** Interface – ethernet1/12 選択で Ethernet Interface 設定ウインドウ [Interface Type] HA <OK>
HA を設定	

`# set deviceconfig high-availability enabled yes`
 	
`# set deviceconfig high-availability group 1 mode active-passive`
 	
`# set deviceconfig high-availability group 1 peer-ip 1.1.1.1`
 	
`# set deviceconfig high-availability group 1 peer-ip-backup 2.2.2.1`
 	
`# set deviceconfig high-availability group 1 configration-synchronization enabled yes`
 	
`# set deviceconfig high-availability group 1 election-option device-priority 10`
 	
`# set deviceconfig high-availability interface ha1 port dedicated-ha1 ip-address 1.1.1.2 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha1-backup port ethernet1/12 ip-address 2.2.2.2 netmask 255.255.255.0`
 	
`# set deviceconfig high-availability interface ha2 port dedicated-ha2`
	[Device]＞[High Availability]＞[General]タブ画面
	・Setup 設定ウインドウ
	[Enable HA]にチェック
	[Group ID] 1
	[Mode] Active Passive
	[Peer HA1 IP Address] 1.1.1.1
	[Backup Peer HA1 IP Address] 2.2.2.1
	[Enable Config Sync]にチェック
	<OK>
	
	・Election Settings 設定ウインドウ
	[Device Priority] 10
	<OK>
	
	・Control Link(HA1) – Primary 設定ウインドウ
	[Port] dedicated-ha1(Dedicated out of band HA1 interface)
	[IP Address] 1.1.1.2
	[Netmask] 255.255.255.0
	<OK>
	
	・Control Link(HA1) – Backup 設定ウインドウ
	[Port] ethernet1/12
	[IP Address] 2.2.2.2
	[Netmask] 255.255.255.0
	<OK>
	
	・Data Link(HA2)設定 – Primary 設定ウインドウ
	[Port] dedicated-ha2(Dedicated out of band HA2 interface)
	<OK>

リンクモニタリングの設定	

`#set deviceconfig high-availability group 1 monitoring link-monitoring link-group toAX interface [ ethernet1/23 ethernet1/24 ]`
 	
`#set deviceconfig high-availability group 1 monitoring link-monitoring link-group toAX enabled yes`
 	
`#set deviceconfig high-availability group 1 monitoring link-monitoring link-group toAX failure-condition all`
	[Device]＞[High Availability]＞[Link and Path Monitoring]タブ画面
	・[Link Group]にて[Add] – Link Group 設定ウインドウ
	[Name] toAX
	[Enabled]にチェック
	[Failure Condition] all
	[Interfaces▲] ethernet1/23, ethernet1/24 を Add
	<OK>

設定内容の反映	
`# commit`	画面右上  をクリック

以上の設定終了後、アクティブ装置へ接続します。

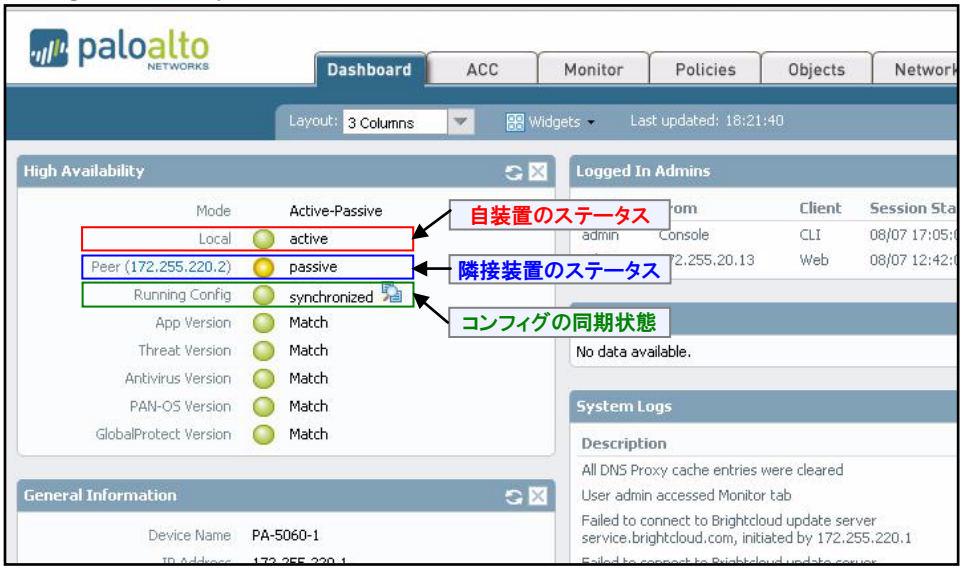
Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

パッシブ側の装置については、アクティブ側の装置でおこなった設定をおこなう必要はなく、アクティブ装置とコンフィグの同期をおこなえば OK です。

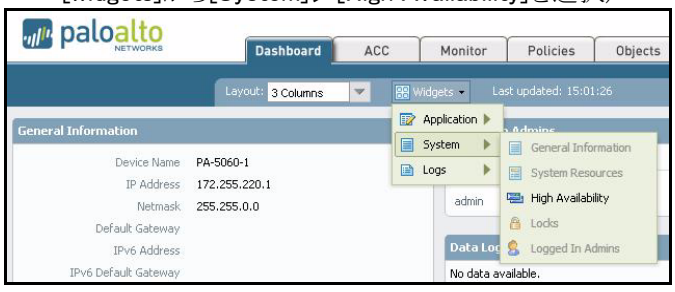
FW1 (PA-5060:アクティブ側) の設定	
CLI	GUI
HA の同期	
実行コンフィグの同期	
`> request high-availability sync-to-remote running-config`	[Dashboard]タブ＞[HighAvailability]ウィジェット [Running Config]の項、sync to peer 横の Sync to peer をクリック

HA の確認は以下の通りです。

GUI の場合
[Dashboard]＞[High Availability]



※[Dashboard]に[High Availability]ウィジェットが無い場合は、
[widgets]から[System]＞[High Availability]を選択）



Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

CLI の場合

```
# show high-availability state

Group 1:
  Mode: Active-Passive
  Local Information:                                          自装置の情報
    Version: 1
    Mode: Active-Passive
    State: active                 自装置のステータス
    Device Information:
      Management IP Address: 172.255.0.10; Netmask: 255.255.0.0
      Jumbo-Frames disabled; MTU 1500
    HA1 Control Links Joint Configuration:
      Encryption Enabled: no
    Election Option Information:
      Priority: 10
      Preemptive: no
    Version Compatibility:
      Software Version: Unknown
      Application Content Compatibility: Unknown
      Threat Content Compatibility: Unknown
      Anti-Virus Compatibility: Unknown
      VPN Client Software Compatibility: Unknown
      Global Protect Client Software Compatibility: Unknown
    State Synchronization: not synchronized; type: ethernet
  Peer Information:                                           隣接装置の情報
    Connection status: down       隣接装置の接続状況
    Connection down reason: Never able to connect to peer
    Version: 0
    Mode: Unknown
    State: unknown                隣接装置のステータス
    Device Information:
      Management IP Address:
      Connection down; Reason: Never able to connect to peer
      Connection down; Reason: Never able to connect to peer
    Election Option Information:
      Priority: 100
      Preemptive: no
  Configuration Synchronization:
    Enabled: yes
    Running Configuration: unknown    コンフィグの同期状態
```

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

4. 効率的な運用ツール

仮想化されたネットワークはその構成が物理的な構成、いわゆる見た目の構成と異なることが多くなり、運用管理の面で負担が大きくなりがちです。

アラクサラのネットワーク・パーティションやパロアルトネットワークス PA シリーズでは、仮想化によって複雑になりがちなネットワークの運用を手助けするツールも用意されています。

4.1 AX-Networker's Utility（仮想ネットワーク可視化ツール）

AX-Networker's-Utility（仮想ネットワーク可視化ツール）は，ネットワーク上に存在する装置の VRF/VLAN コンフィグレーションを集中的に収集，一覧表示し，その設定内容をチェックできるツールです。
また，ネットワーク上に存在する装置に接続された装置や端末の情報（以下，リソース情報）を集中的に収集，一覧表示し，検索できます。

- 装置の VRF/VLAN コンフィグレーションを収集し，装置間の VRF/VLAN コンフィグレーションを確認，検索および整合性チェックすることができます。

- 装置のリソース情報を収集し，その収集時点で装置に接続されている装置や端末の情報を確認できます。リソース情報としては，装置に接続している装置や端末の台数，装置や端末の MAC アドレス，Web 認証ログイン済み端末の IP アドレス，Web 認証ログイン済みユーザ名，論理名，Web/MAC 認証ログイン経過時間，Web/MAC 認証ログイン残時間，装置や端末が接続されている装置側のポート番号を一覧表示します。

- 装置の VRF/VLAN コンフィグレーションやリソース情報の収集を，GUI を利用して簡単に実施できます。広域・多拠点に分散する収集対象装置の台数が多い場合に，作業者の負荷を軽減できます。

これにより，装置の VRF/VLAN コンフィグレーションを更新する際に VRF/VLAN コンフィグレーションの整合性チェックを行ったり，装置のリソース情報を収集して，装置に接続されている装置や端末を VRF や VLAN 毎に接続されている台数として確認したり，特定のリソース情報のキーワードによる検索が容易に行えるようになります。

図 4.1-1 AX-Networker's Utility(仮想ネットワーク可視化ツール) 参照画面例

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

4.2 Panorama(集中セキュリティ管理システム)

パロアルトネットワークスの Panorama は、グローバルな可視性を提供し複数のファイアウォールの制御を可能にする集中セキュリティ管理システムです。一つのアプリケーションから複数のファイアウォールを包括的、もしくはデバイス個別にアプリケーションやユーザ、ネットワークに流れるデータまで管理できます。

それに加え、集中ポリシー管理、ファイアウォールの容易な導入とアップデート、集中ロギング及びレポーティング、ログストレージと高可用性などの特長も持ち合わせています。

図 4.2-1Panorama 使用イメージ

Panorama で使用できる代表的な機能をいくつか紹介します。

Application Command Center (ACC): ネットワーク上のアプリケーションの通信をセッションごと、バイト数、ポート番号、脅威の有無及び時間などをビジュアルに可視化します。管理者はマウスによって簡単に設定できるフィルター機能を利用することによってネットワークでなにが行われているのかを理解することができます。

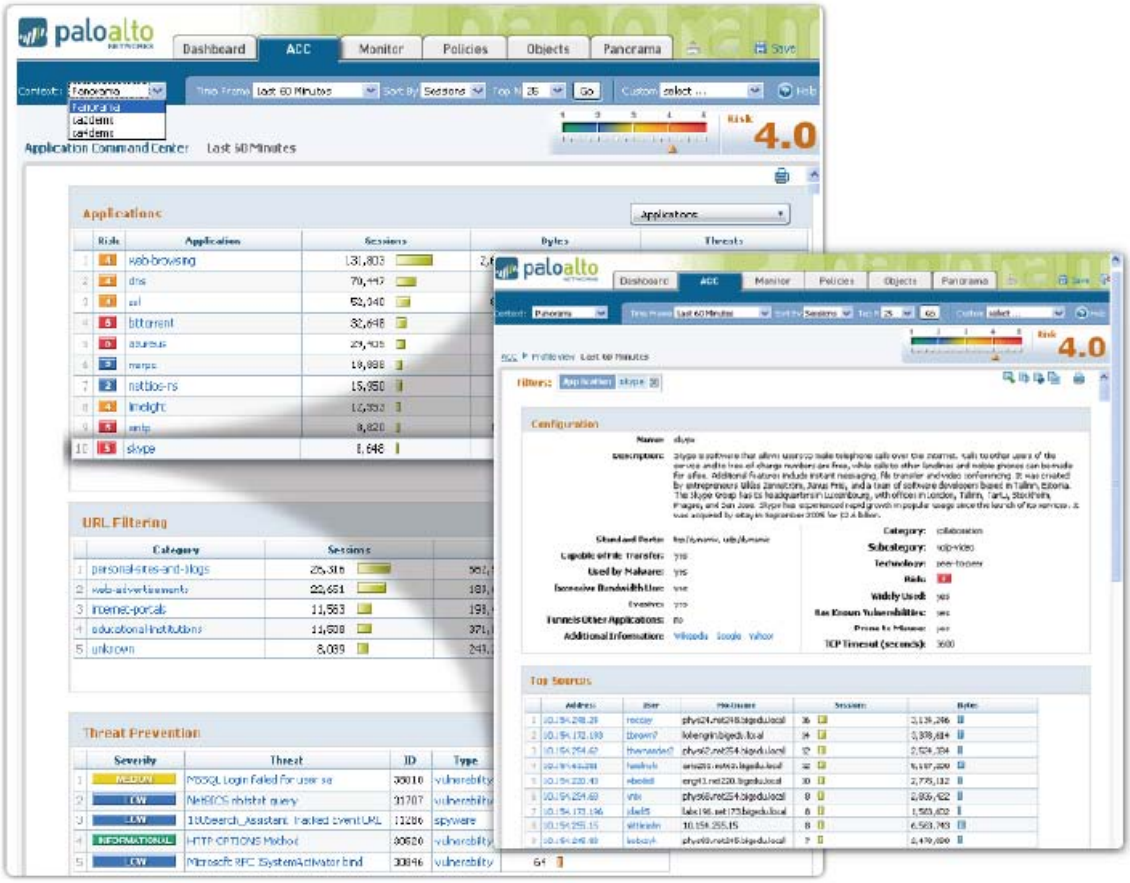


図 4.2-2 Application Command Center

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

アプリケーションブラウザ: アプリケーションブラウザを使うと管理者はアプリケーション毎のカテゴリ、目的、使われている技術、主な動作の特徴などの様々な情報にダイナミックにアクセスすることができます。

共有ポリシー: 共有ポリシーにより、管理者はローカルルールの上位にベースとなるポリシーを設定でき、管理労力の削減とポリシーの一貫性の向上につなげることができます。共有ポリシーは、より詳細なロールベースの管理機能により補完されます。

図 4.2-3 共有ポリシー

ロギング: 詳細なログはそれぞれのファイアウォールで取得します。それぞれのフィールドに対するフィルターや任意のパターンマッチにより選別することが可能です。

レポーティング: 30 種以上の予め定義されたレポーティング機能を使うこともできますし、カスタマイズすることも可能です。レポートは PDF 形式に変換され、定期的にメールによって配信することが可能です。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

5. 留意事項

(1) Aggregate Ethernetインタフェースはスタティックリンクアグリゲーション相当

パロアルトネットワークス PA シリーズの Aggregate Ethernet インタフェースはスタティックリンクアグリゲーション相当の機能であり、LACP モードはサポートされません。従って AX シリーズとリンクアグリゲーションを使って接続する場合はスタティックモードを使用してください。

(2) VSYS使用時のIPアドレス付与について

パロアルトネットワークス PA シリーズにおける Layer3 設定のインタフェース(Ethernet, VLAN 等)は、異なる VSYS に属していてもホストアドレスまで全く同じ値の IP アドレスを与えることはできません。但しホストアドレスさえ異なれば、同一のアドレスブロック(ネットワークアドレス)とすることは可能です。

例: VLAN10 に 10.0.0.10 / VLAN20 に 10.0.0.10 → 不可
VLAN10 に 10.0.0.10 / VLAN20 に 10.0.0.11 → OK

(3) HA構成時のコンフィグ同期について

複数装置による冗長構成、いわゆる HA 構成とする場合、論理的に矛盾のないようコンフィグ等の設定も装置間で一致させておく必要がありますが、パロアルトネットワークス PA シリーズでは HA 構成の装置間にてコンフィグを同期させる機能があります。
ただしコンフィグ同期は自動的におこなわれませんので、コンフィグを同期させる際はアクティブ側装置(コンフィグ同期元装置)での Web のコンフィグ同期指示もしくは CLI での同期コマンド実行、あるいは commit 実行をおこなってください。

(4) パロアルトネットワークスPAシリーズでのコンフィグ保存について

パロアルトネットワークス PA シリーズでのコンフィグの保存は、GUI における操作で[Device]＞[Operation]からできますが、装置外への保存(Export)をおこなう際、保存される(ダウンロードされる)ファイルは xml 形式のテキストで保存されます。CLI 操作でのいわゆる流し込みに対応したファイルが必要な場合には、CLI 操作にて「set cli config-output-format set」コマンド実行後の「show」コマンド(※)出力を保存すると良いでしょう。

```
admin@PA-5060(active)# show
deviceconfig {
  system {
    ip-address 172.255.0.10;
    netmask 255.255.0.0;
    update-server updates.paloaltonetworks.com;
    update-schedule {
      threats {
        recurring {
          weekly {
              :

admin@PA-5060(active)> set cli config-output-format set
admin@PA-5060(active)> configure
Entering configuration mode
[edit]
admin@PA-5060(active)# show
set deviceconfig system ip-address 172.255.0.10
set deviceconfig system netmask 255.255.0.0
set deviceconfig system update-server updates.paloaltonetworks.com
set deviceconfig system update-schedule threats recurring weekly
day-of-week wednesday
              :
```

※set cli config-output-format set の適用はコンフィグモードでの show コマンド表示に対応します。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

付録

本ガイドにて紹介した構成のコンフィグレーション例です。

3 章の各ネットワーク構成における各装置の全コンフィグレーションについて、テキスト形式のファイルとして本ファイルに添付しております。(添付ファイルを抽出するには、Adobe Acrobat 5.0 以降もしくは Adobe Reader 6.0 以降が必要です。)

各コンフィグレーションについては、以下に示すファイル名と同じ名前の添付ファイルを参照下さい。

3.1 FTスイッチ + PAシリーズHA構成の例

	装置名と対象装置	対象ファイル
L3 コアスイッチ	C1 (AX6604S)	3-1_AXPA-guide_FT_C1.txt
ファイアウォール(*1)	FW1(PA-5060)	3-1_AXPA-guide_FT_FW1.xml
L2 アクセススイッチ	S1 (AX2530S-24T4X)	3-1_AXPA-guide_FT_S1.txt
	A1 (AX1240S-24T2C)	3-1_AXPA-guide_FT_A1.txt
	A2 (AX1240S-24T2C)	3-1_AXPA-guide_FT_A2.txt

(*1)FW のコンフィグは HA のアクティブ分のみです。パッシブ側のコンフィグは HA 構成後アクティブと同期させてください。

3.2 スタック + PAシリーズHA構成の例

		装置名と対象装置	対象ファイル
L3 コアスイッチ	スタック移行用(*1)	(ﾏｽﾀｽｲｯﾁ:AX3560S-24T6XW)	MST_AX36S.txt
		(ﾊﾞｯｸｱｯﾌﾟｽｲｯﾁ:AX3560S-24T6XW)	BAK_AX36S.txt
	スタック移行後	C1 (AX3650S-24T6XW ｽﾀｯｸ)	3-2_AXPA-guide_STK_C1.txt
ファイアウォール(*2)		FW1(PA-5060)	3-2_AXPA-guide_STK_FW1.xml
L2 アクセススイッチ		S1 (AX2530S-24T4X)	3-2_AXPA-guide_STK_S1.txt
		A1 (AX1240S-24T2C) (*3)	(3-1_AXPA-guide_FT_A1.txt)
		A2 (AX1240S-24T2C) (*3)	(3-1_AXPA-guide_FT_A2.txt)

(*1)スタックを構成するコアスイッチでは、スタックに移行する前のコンフィグレーションファイル(マスタ/バックアップ各スイッチ用)も添付しています。

(*2)FW のコンフィグは HA のアクティブ分のみです。パッシブ側のコンフィグは HA 構成後アクティブと同期させてください。

(*3)装置 A1 および A2 のコンフィグは、「3.1 FT スイッチ+PA シリーズ HA 構成の例」のものと共通となります。

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

〈空白ページ〉

Copyright © 2013, ALAXALA Networks Corporation. All rights reserved.

2013 年 3 月 15 日　初版発行
資料 No. NTS-12-R-039

アラクサラネットワークス株式会社
ネットワークテクニカルサポート

〒212-0058
川崎市幸区鹿島田 1 丁目 1 番地 2 号　新川崎三井ビル西棟
http://www.alaxala.com/