ICTの力を、お客様のビジネスの推進力に。

Your ICT Force

ハードウェア アプライアンスでの仮想化

2009年11月26日
Internet Week 2009

大須賀 怜
(日本UNIXユーザ会)

UNIADEX
ユニアデックス株式会社

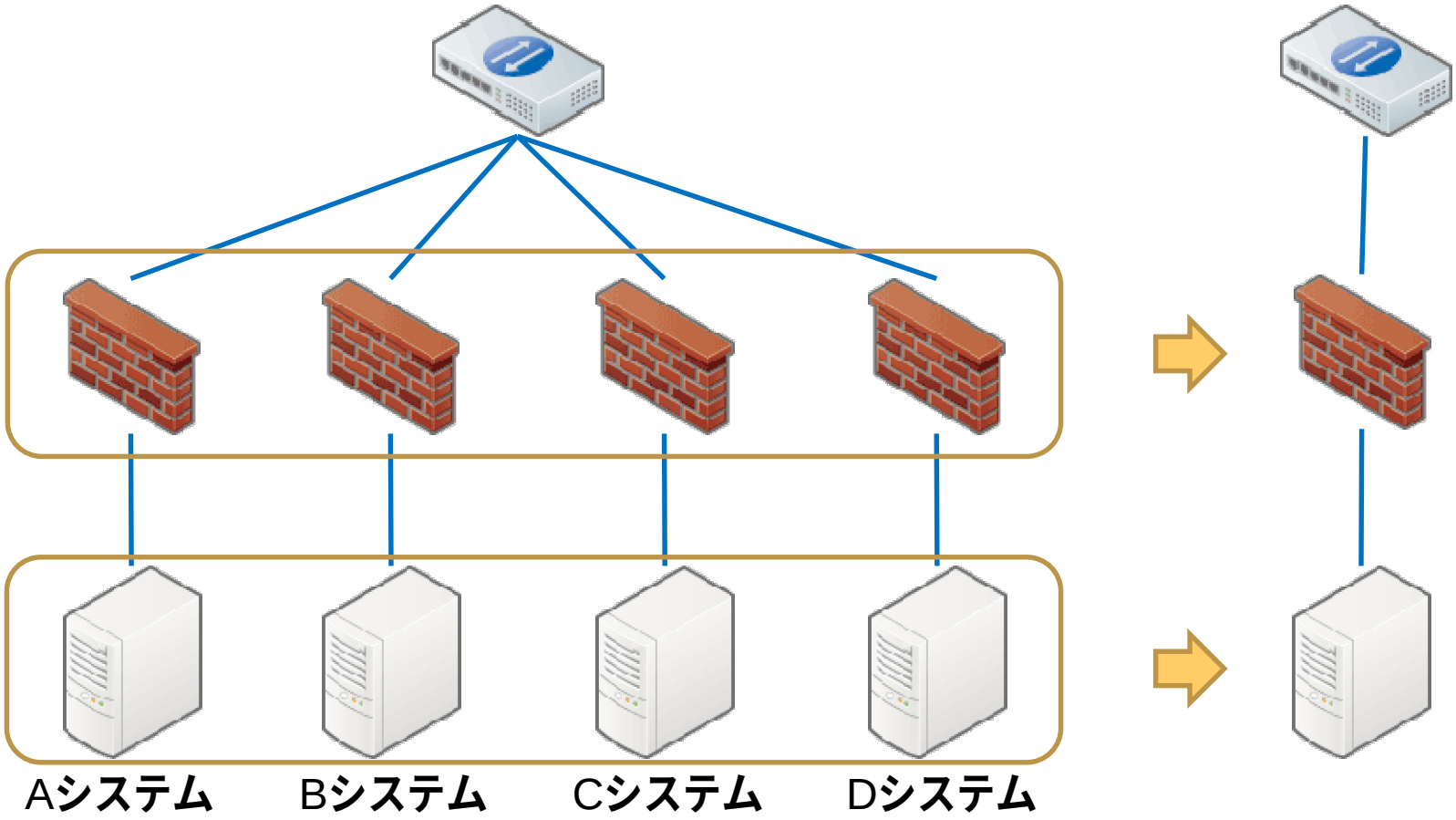
はじめに

- サーバの仮想化は身近なものになりました
- ネットワーク機器にも仮想化技術は取り入れられていってます
  - しかし、NW屋さん以外には「ネットワークの仮想化と言われてもイメージがわかない」と言われがち
  - 実はVLAN(Virtual LAN)、VPN(Virtual Private Network)、VRRP(Virtual Router Redundancy Protocol)等々、意外と身近にありますが、さすがにこれらは今更御説明するまでも無いでしょう
- 今回は〝ハコ〞の中での仮想化に焦点を絞り、いま現場で使われている仮想化技術について御紹介します

All rights Reserved, Copyright©2009 UNIADEX, Ltd.

例1 - ファイアウォールの仮想化

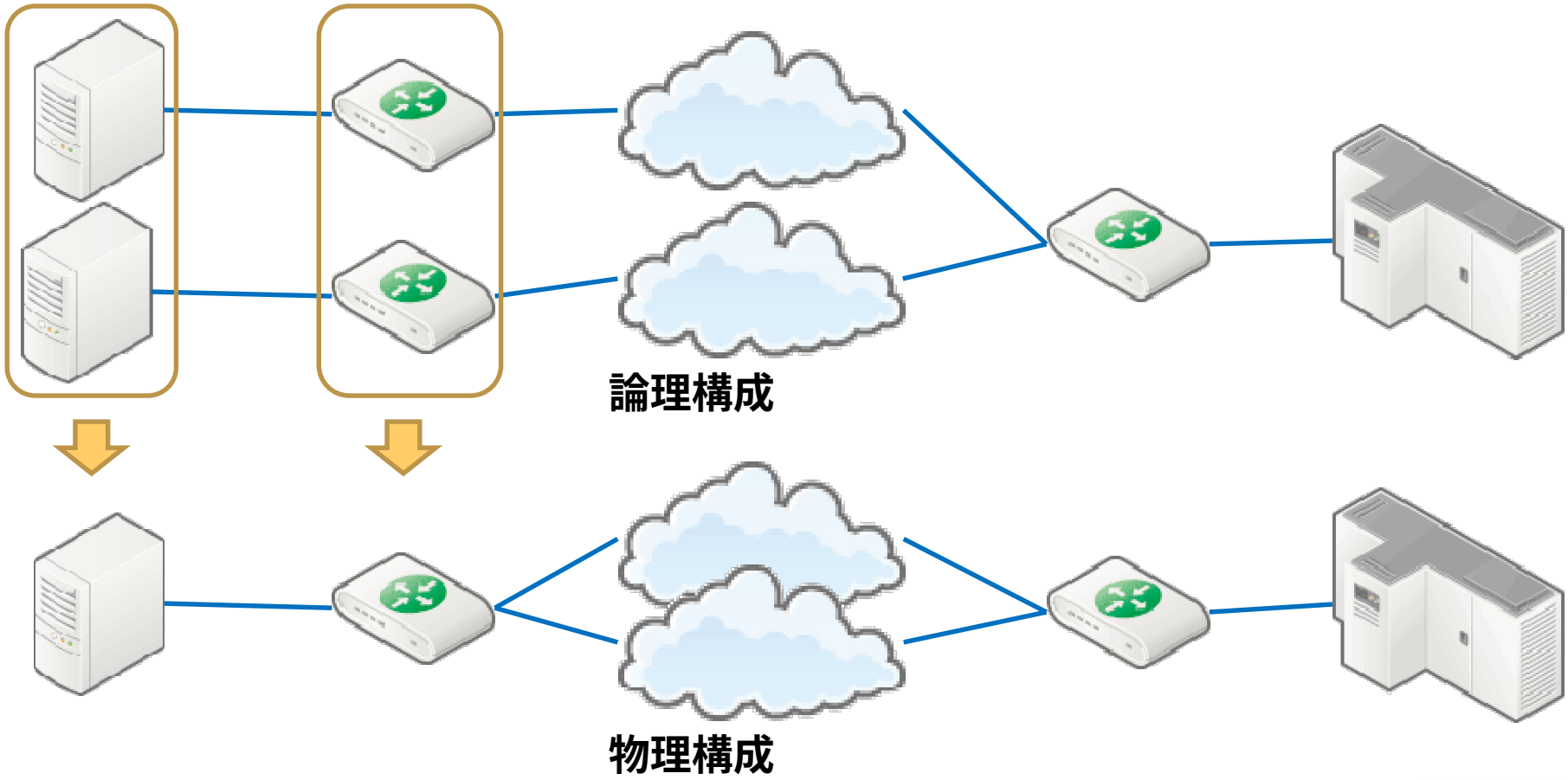
- システムごとに存在するファイアウォールを全て仮想ファイアウォールに！
  - 1つのファイアウォールでフィルタを工夫してシステムを分離するという手段もあるが、フィルタの複雑化や、考慮漏れ等による不正な通信の成立が有り得る



All rights Reserved, Copyright©2009 UNIADEX, Ltd.
UNIADEX

例2 - ルーティングテーブルの仮想化

- 1つのルータで複数のルーティングテーブルを！
  - ルーティングテーブル以外は共用
  - 従来はPBRにより送信元ベースのルーティングにして実現していたケースの幾らかは、宛先ベースのルーティングのみで実現可能になります



All rights Reserved, Copyright©2009 UNIADEX, Ltd.
UNIADEX

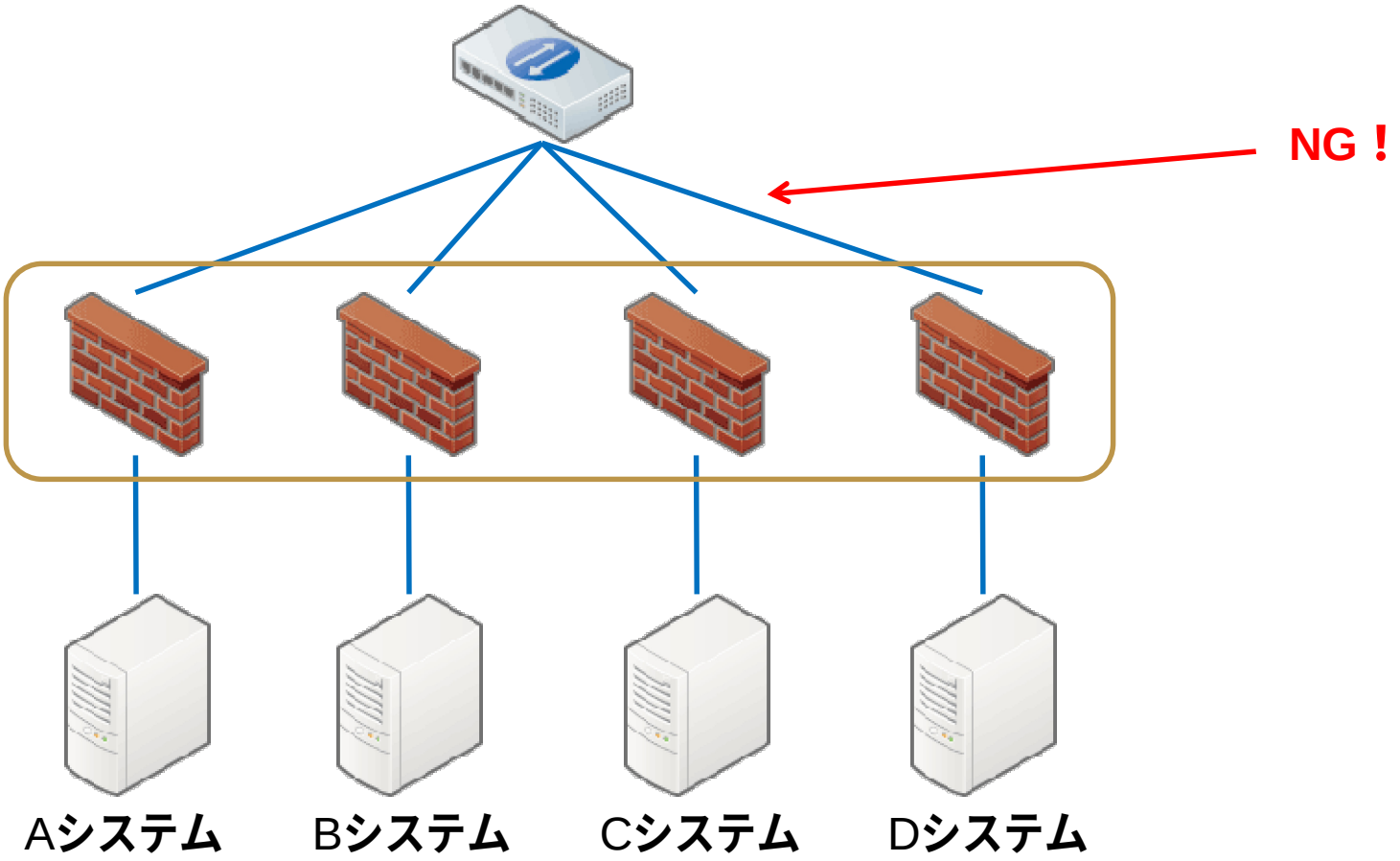
落とし穴！

- 一見単純な仕組みの仮想化ですが、仮想システムにはプロダクト毎の様々な制限が発生します
  - 使えない機能が出てくる
    - IPv6に非対応だったり
    - ダイナミックルーティングに非対応だったり
    - VPNには非対応だったり
    - etc...
  - 作りが甘くてバグが出る
    - 他の仮想システムのリソースにアクセスできてしまったり
    - あるシステムでの不正な操作で全仮想システムがクラッシュしてしまったり
  - 運用が大変になる事も
    - ハードウェア交換の際には全仮想システムでリストア作業が必要になったり
    - pingやtracerouteでルーティングテーブルの指定が必須だったり
    - あるシステムのみOSのバージョンを変える、という事ができなかったり
  - 想像の及ばない細かい細かい仕様でハマる事も
  - 設計ポリシーの都合で仮想化が適さない事も

All rights Reserved, Copyright©2009 UNIADEX, Ltd.

細かい仕様の都合でハマッた例

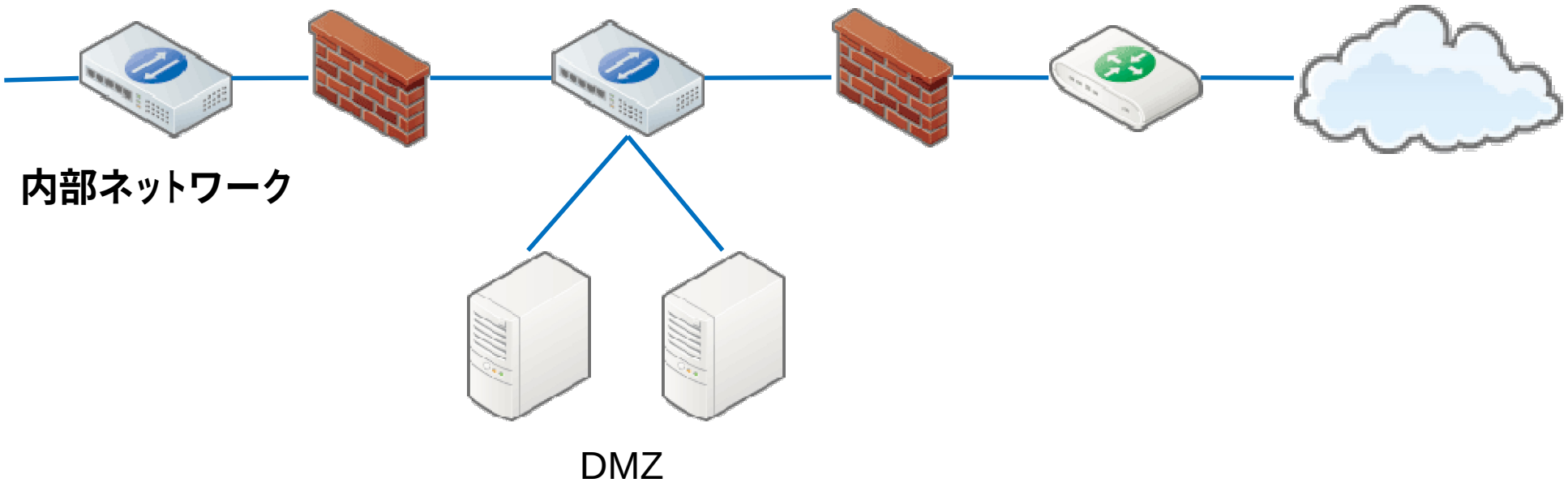
- 仮想システムは沢山作れるが、VLAN IDで通信を振り分ける仕組みだった！
  - 1つのVLANに2つ以上の仮想システムを作れなかった、なんて事がありました



All rights Reserved, Copyright©2009 UNIADEX, Ltd.

設計ポリシーの都合で仮想化できなかった例

- DMZを構成する2つのファイアウォールを物理的には1つに・・・しようとしたのだが
  - "2つのファイアウォールは異ベンダの製品である事"というポリシーにより断念



All rights Reserved, Copyright©2009 UNIADEX, Ltd.

商用サービスの事例紹介

会場ONLY

All rights Reserved, Copyright©2009 UNIADEX, Ltd.

まとめ

- 単純に沢山のハコが物理的に1つになる、と言うほどには簡単に動かない
  - プロダクト毎の実装であるため、ハマりどころが様々
  - まずは使いたい機能が仮想システム上でも使えるのかを確認する事が必須
- ちゃんとノウハウさえ持っていれば、品質的には商用環境で十分使えるレベルのものが市場に出てきている

NWアプライアンスでも仮想化、できます！

All rights Reserved, Copyright©2009 UNIADEX, Ltd.

UNIADEX

Your ICT Force

講師自己紹介

- 氏名 ・・・ 大須賀 怜 (おおすが さとし)
- 所属 ・・・ ユニアデックス株式会社
  ビジネスイノベーション統括部 プラットフォームマーケティング部
  技術企画支援グループ
- お仕事 ・・・ ネットワークの新規技術/新プロダクトの開拓･評価と、それらを用いた案件での設計/構築サポート

- ルータとかスイッチとか、ファイアウォールとかロードバランサとか、所謂ハコモノを扱う人
- コンソールでコマンドを叩く系の作業が一番好きで、一応CCIE#17223
- 自宅にルータやスイッチ等がゴロゴロ
- 最近はデータセンタ関係を中心に、仮想化･IPv6等のキーワードに関わるネットワークを主に作ってます

All rights Reserved, Copyright©2009 UNIADEX, Ltd.