radware
availability | performance | security

LinkProofのご紹介

Smart Network. Smart Business.

radware | アジェンダ

- アジェンダ
  - LinkProof概要
  - LinkProofの基本機能
  - LinkProofの動作
  - LinkProofのアドバンスド機能
  - LinkProof導入シナリオ

LinkProof概要

Smart Network. Smart Business.

radware | LinkProof概要

Smart Network. Smart Business.

- LinkProofとは？
  - LinkProofは、複数回線のロードバランス（負荷分散）を インテリジェントに行うことができるアプリケーションスイッチ
- LinkProofを導入することで、インターネットの接続性に対して アベイラビリティ・パフォーマンス・セキュリティを向上

- トラフィックが送信される回線は、ヘルスチェックをパスした回線の中から選ばれるため、可用性（アベイラビリティ）が向上します

- 複数回線をActive-Activeの状態で使用することができるため、パフォーマンスが向上します

- Secure SynAppsライセンスを追加することで、IPS機能を持たせることも可能になり、セキュリティの向上に寄与します

LinkProofの基本機能

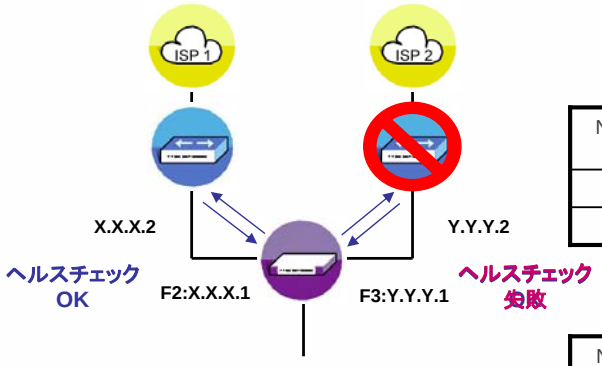
Smart Network. Smart Business.

radware | LinkProofの基本機能

Smart Network. Smart Business.

- LinkProofの基本機能
  - LinkProofは、以下の3つの基本機能を使用することで、回線負荷分散を実現しています
    - ヘルスチェック機能
    - 負荷分散機能
    - NAT機能

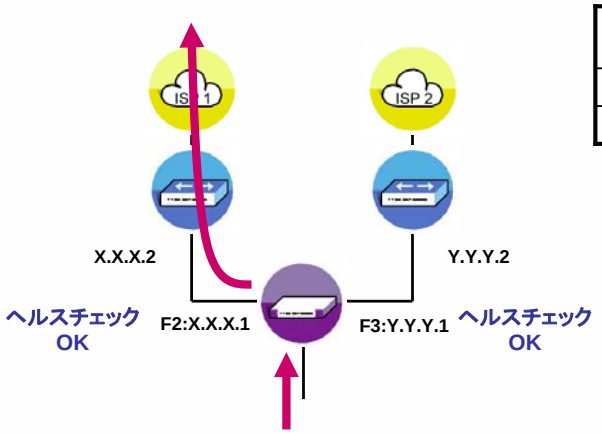
- ヘルスチェック機能
  - どの回線が利用可能かをチェックする機能
    - 回線を収容しているルータをNHR（Next Hop Router）として登録し、そのNHRに対して、Ping等のリクエスト パケットを送信してリプライが返ってきたら、その回線はUpしていると判断する



NHR Address	NHR Name	Operational Status
X.X.X.2	ISP1	Active
Y.Y.Y.2	ISP2	Active

NHR Address	NHR Name	Operational Status
X.X.X.2	ISP1	Active
Y.Y.Y.2	ISP2	notInService

- 負荷分散機能
  - ヘルスチェックをパスしたNHRの中から、どのNHR（ISP回線）を経由してトラフィックを送信するのかを、負荷分散アルゴリズムに基づいて決定する機能



NHR Address	NHR Name	Operational Status
X.X.X.2	ISP1	Active
Y.Y.Y.2	ISP2	Active

負荷分散
アルゴリズム

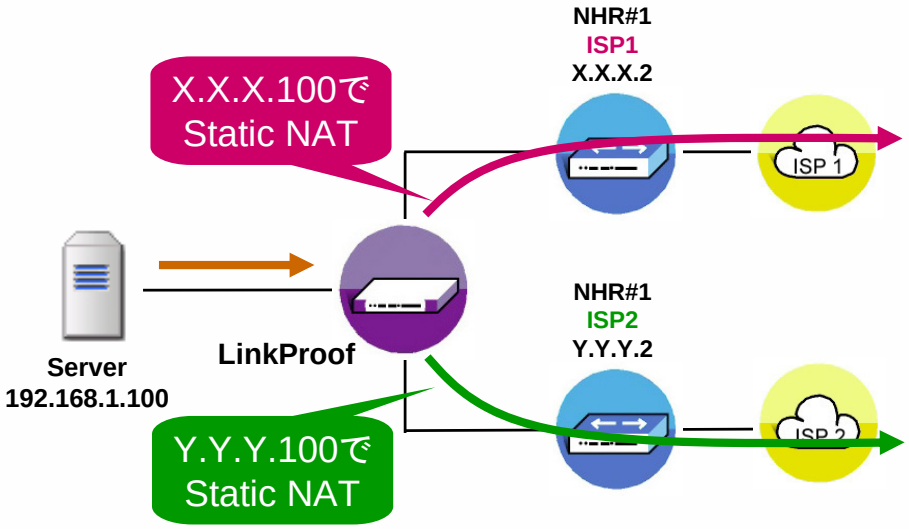
LB
decision

ISP1を使用

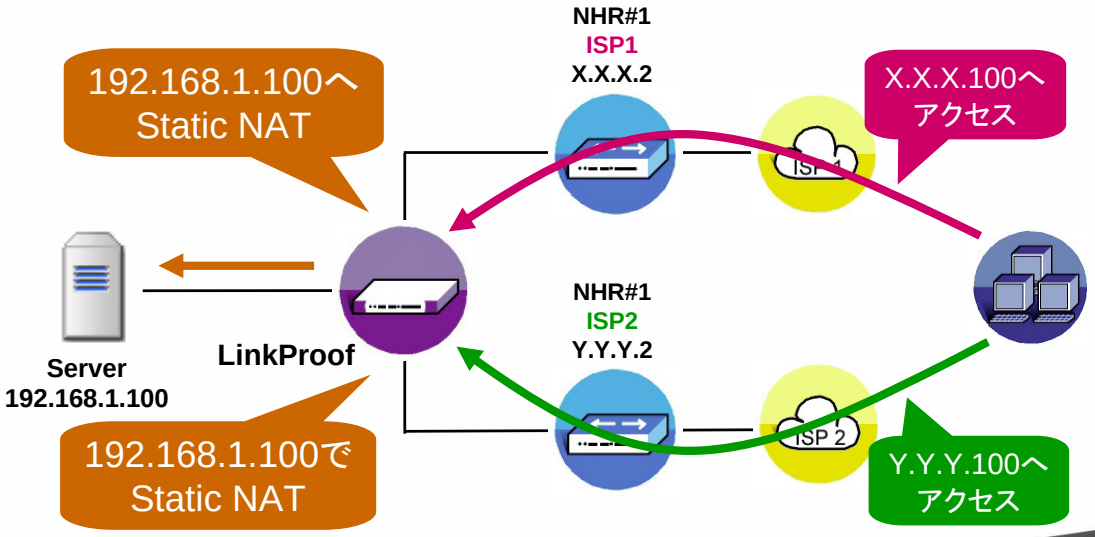
- 負荷分散機能
  - 主要な負荷分散アルゴリズム
    - Cyclic
      - Round Robin
    - Fewest Number of Users
      - NHR毎にセッション数を見て、少ないNHRにトラフィックを振る
    - Least Amount of Traffic
      - NHR毎にppsを見て、少ないNHRにトラフィックを振る
    - Least Number of Bytes
      - NHR毎にBytesを見て、少ないNHRにトラフィックを振る
    - Hashing
      - Source IP、Destination IPを元にハッシュした結果に基づいて、トラフィックを振るNHRを決定する

- NAT機能
  - LinkProofはNATを用いることにより、マルチホーミング（複数回線の負荷分散）を可能にしています
  - LinkProofは以下のタイプのNATをサポートします
    - Static NAT
    - Dynamic NAT
    - No NAT
    - Basic NAT

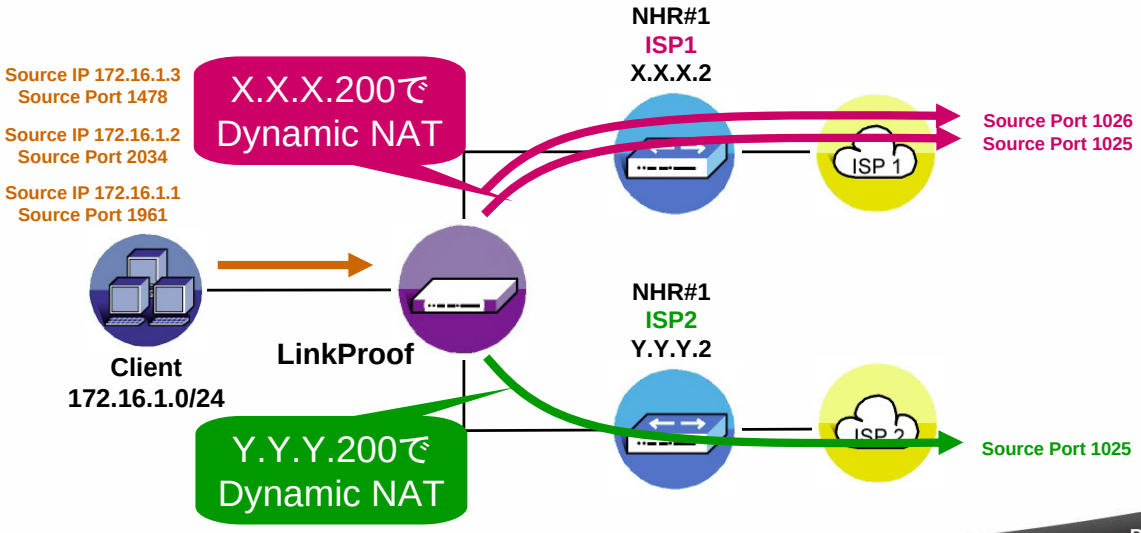
- NATの種類
  - Static NATとは
    - 一対一のNAT
      - 公開サーバが使用するNAT



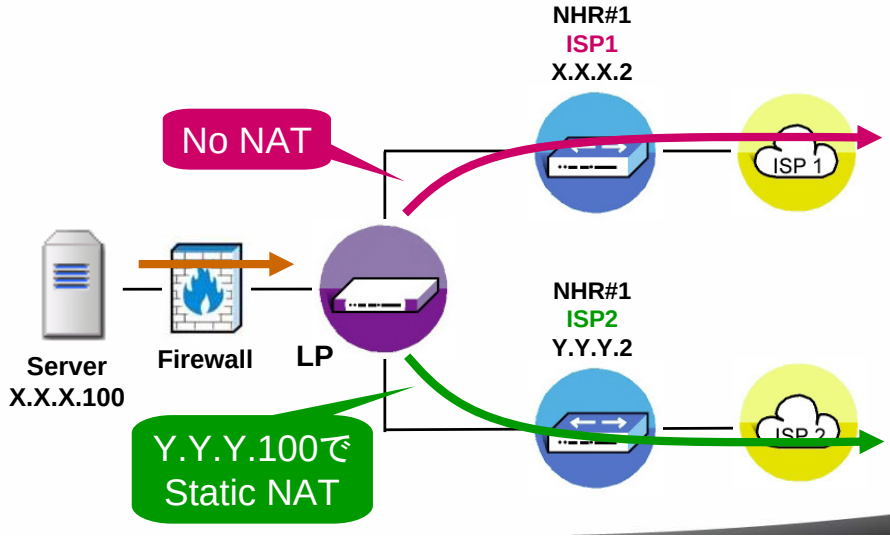
- NATの種類
  - Static NATとは
    - Static NATアドレスは、公開サーバに対する外部ユーザからのアクセスにも使われます



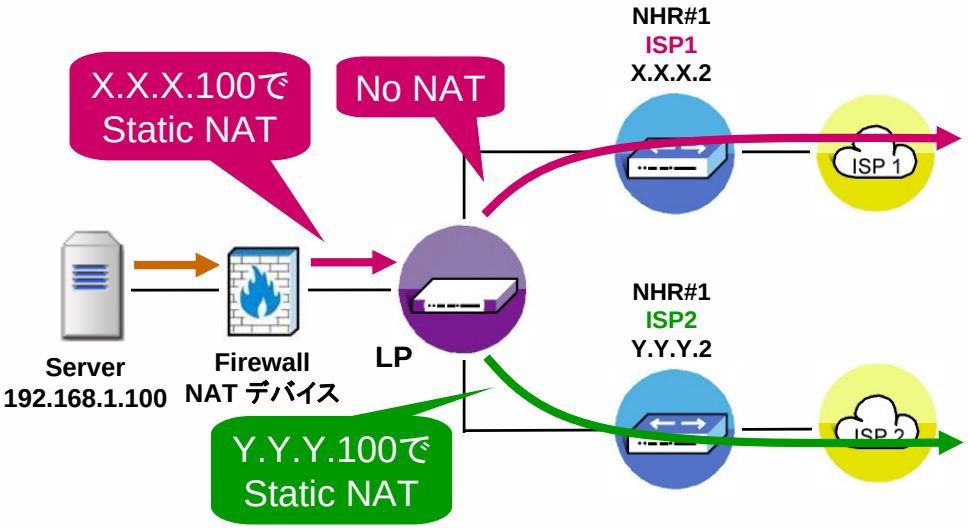
- NATの種類
  - Dynamic NATとは
    - PATを使用した多対一のNAT
      - クライアントのインターネットアクセスのために使用するNAT



- NATの種類
  - No NAT
    - NATを使用しない
      - グローバルアドレスが既に付加されている公開サーバに対して、NATせずにインターネットに出て行く場合に使用するNAT



- NATの種類
  - No NAT
    - NATを使用しない
      - 他にNATデバイスがあり、LinkProofでNATをする必要がない場合に使用する

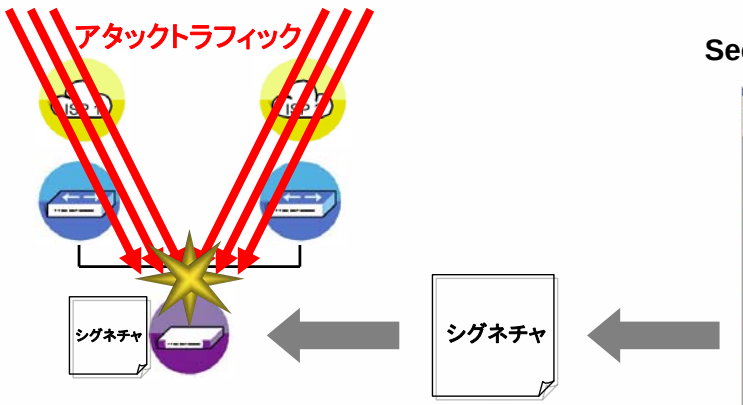


- NATの種類
  - Basic NAT
    - NAT アドレスのプールを作成し、そのアドレスを使用して Static NATをします
      - ソースポートを変更したくないアプリケーション（Net meeting等）向けのNAT

- IPS機能（オプション）
  - LinkProofにSecure SynAppsライセンスを追加することで、アタックトラフィックから内部ネットワークを保護することが可能
  - 弊社が提供する既知のアタックに対するシグネチャをLinkProofにアップロードすることで、それにマッチするアタックトラフィックをLinkProofが完璧にブロックします
  - シグネチャは毎週月曜日に更新され、新しい緊急度の高いアタックに対するシグネチャは逐次作成され、提供されます

radware | LinkProofの基本機能
Smart Network. Smart Business.

- IPS機能（オプション）
  - 弊社セキュリティWebページからシグネチャをダウンロードし、LinkProofにシグネチャをアップロードします



www.radware.com
Security Update Serviceページ

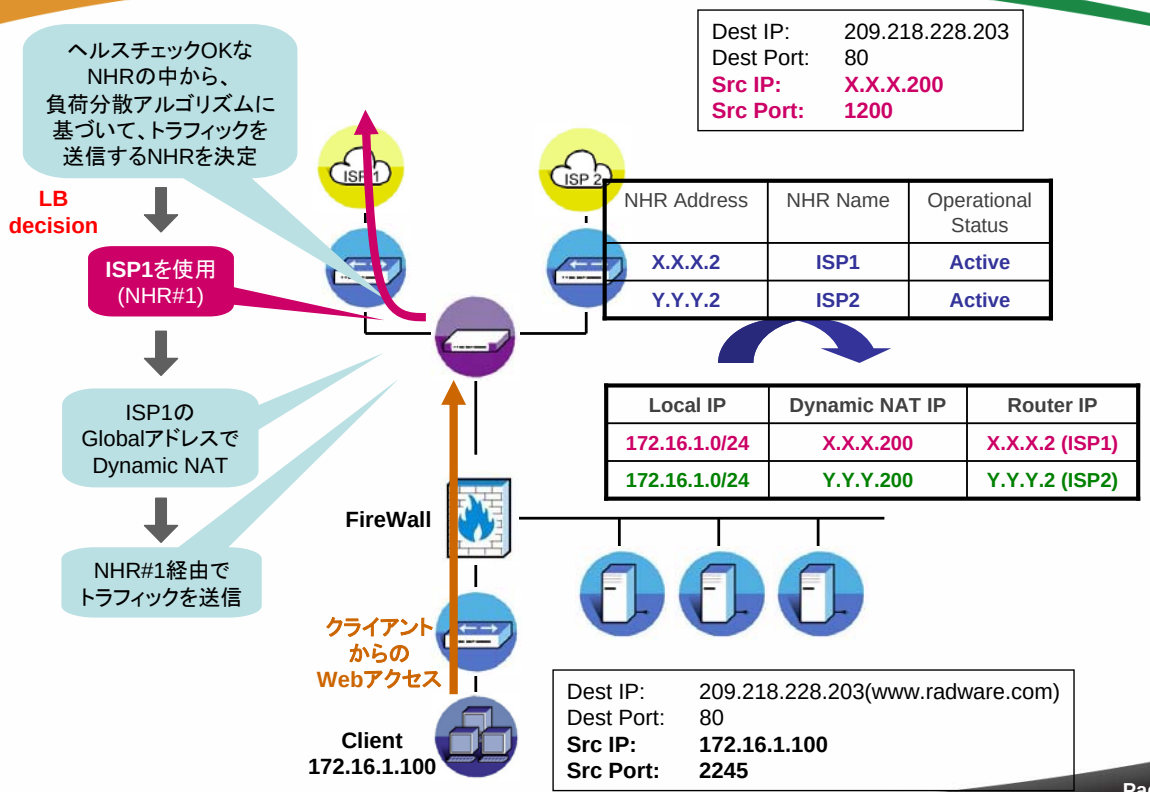
LinkProofの動作

Smart Network. Smart Business.

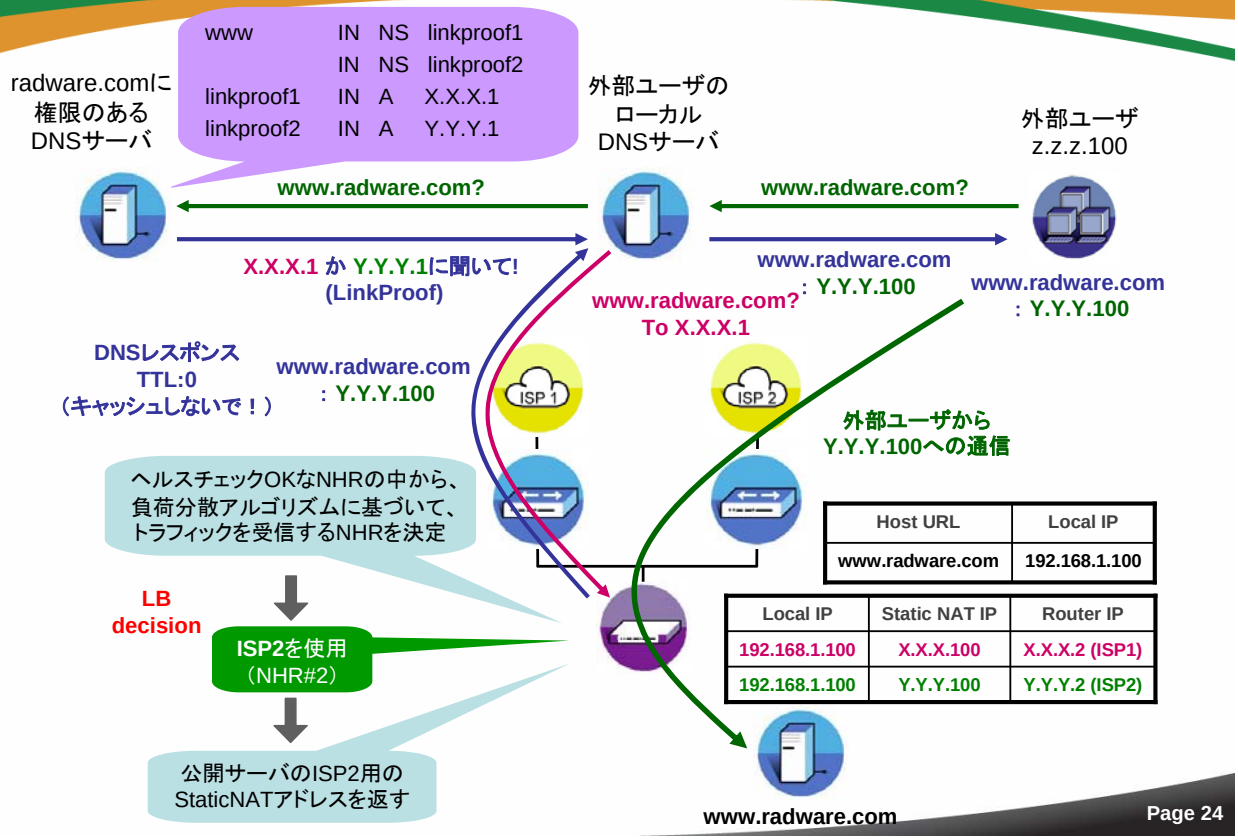
- LinkProofの動作
  - LinkProofは、これまで説明した基本機能を用いることで、アウトバウンド、インバウンドの回線負荷分散を実現しています
    - アウトバウンド トラフィックの負荷分散
      - 負荷分散アルゴリズムに基づいたロードバランス
    - インバウンド トラフィックの負荷分散
      - 負荷分散アルゴリズムに基づいたロードバランス
      - DNSリダイレクション機能
        - » LinkProofをDNSサーバに設定し、LinkProofがDNSクエリを受けたとき、負荷分散アルゴリズムに基づいて、外部からアクセスして欲しい公開サーバのNATアドレス（DNSレスポンス）を返すことにより、インバウンドの負荷分散を実現しています

- アウトバウンド トラフィックの負荷分散
  - LinkProofの基本機能を用いたアウトバウンド トラフィックの動作を、以下のシナリオに基づいて説明します
    - シナリオ
      - ISP1,ISP2による複数回線を持つ
      - ISP1から割り当てられたアドレス　X.X.X.0/24
      - ISP2から割り当てられたアドレス　Y.Y.Y.0/24

radware | LinkProofの動作（アウトバウンド）
Smart Network. Smart Business.



- インバウンド トラフィックの負荷分散
  - LinkProofの基本機能を用いたインバウンド トラフィックの動作を、以下のシナリオに基づいて説明します
    - シナリオ
      - ISP1,ISP2による複数回線を持つ
      - ISP1から割り当てられたアドレス　X.X.X.0/24
      - ISP2から割り当てられたアドレス　Y.Y.Y.0/24
      - ISP1用の公開サーバのアドレス　X.X.X.100
      - ISP2用の公開サーバのアドレス　Y.Y.Y.100
      - LinkProofをDNSサーバとして設定



LinkProofのアドバンスド機能

Smart Network. Smart Business.

- LinkProofのアドバンスド機能
  - 以下の機能を使用することにより、管理者の意図に基づいた
    より詳細なトラフィックの扱いが可能になります
    - NHRの管理
    - 詳細なヘルスチェック
    - グルーピング
    - クライアントテーブル管理
  - 要件により、以下の機能もご使用ください
    - 冗長化
    - 近接性
    - 仮想トンネル

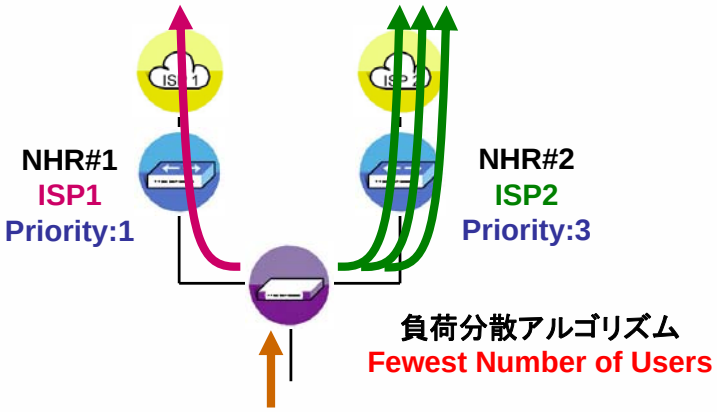
NHRの管理

Smart Network. Smart Business.

- NHRの管理
  - NHR（Next Hop Router）のパラメータを変更することで、NHRへのトラフィックのリダイレクトの仕方を変更することが出来ます
    - NHR Priority
    - NHR Recovery Time & Warm Up Time
    - NHR Connection Limits
    - NHR Operational Mode

- NHR Priority
  - 他のNHRに対して、どれくらいの割合でトラフィックが振られるのかを指定するもの（NHRの重み付け）
  - もし、負荷分散アルゴリズムがFewest Number of Usersに設定されていた場合、NHR Priorityの割合に基づいてトラフィックが振られるセッション数の割合が決まる
  - Priorityは 1-100を設定可能（Defaultは1）
  - 負荷分散アルゴリズムCyclic（Round Robin）と一緒に使うことはできません

- NHR Priority

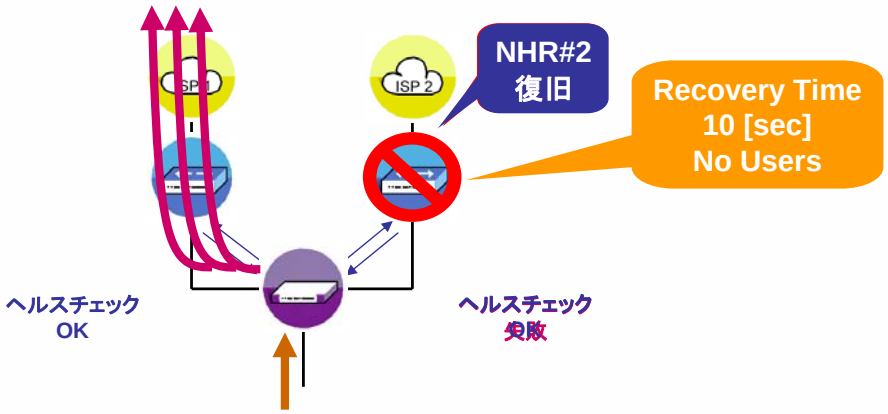


LinkProof # lp next-hop-router table

NHR Address	NHR Name	Operational Status	NHR Priority	Attached Users Number
1.1.1.100	ISP1	active	1	20
2.2.2.200	ISP2	active	3	60

- NHR Recovery Time & Warm Up Time
  - NHRがダウンし、その後復旧した際に、LinkProofがそのNHRに対してどのようにトラフィックを振り始めるのかを設定する
    - Recovery Time（秒：Defaultは0）
      - NHRが復旧したとき（ヘルスチェックOKになったとき）、LinkProofがそのNHRにトラフィックを送る前に、ある期間 待つように設定することができる
      - NHRのブートプロセスを完全に終了させるためのもの

- NHR Recovery Time & Warm Up Time

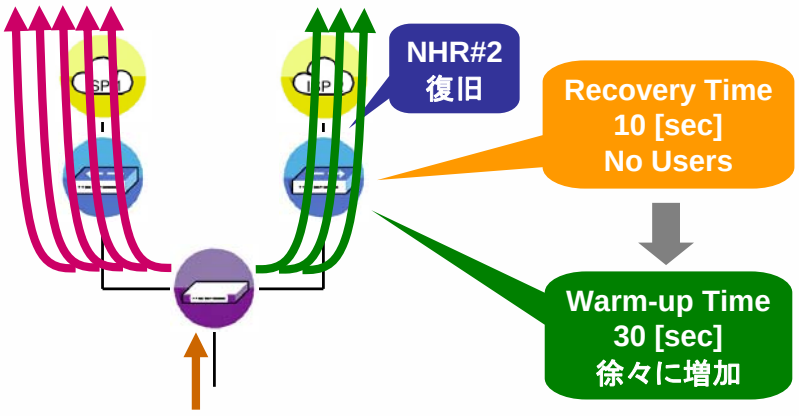


負荷分散アルゴリズム
Fewest Number of Users

復旧したNHRのヘルスチェックがOKになっても、ブートプロセスを完全に終わらせるために Recovery Timeの期間、トラフィックを振らない

- NHR Recovery Time & Warm Up Time
  - Warm-up Time（秒：Defaultは0）
    - Recovery Time終了後、そのNHRに対して、この期間中徐々に振るトラフィックの量を増加させる（内部的には、そのNHRに振られるトラフィックのweightを徐々にあげていく）
    - 負荷分散アルゴリズムがFewest Number of Users等に設定されている場合に、大量のトラフィックが一気にそのNHRに押し寄せてくるのを防ぐ
    - 負荷分散アルゴリズムCyclic（Round Robin）と一緒に使うことはできません

- NHR Recovery Time & Warm Up Time



負荷分散アルゴリズム
Fewest Number of Users

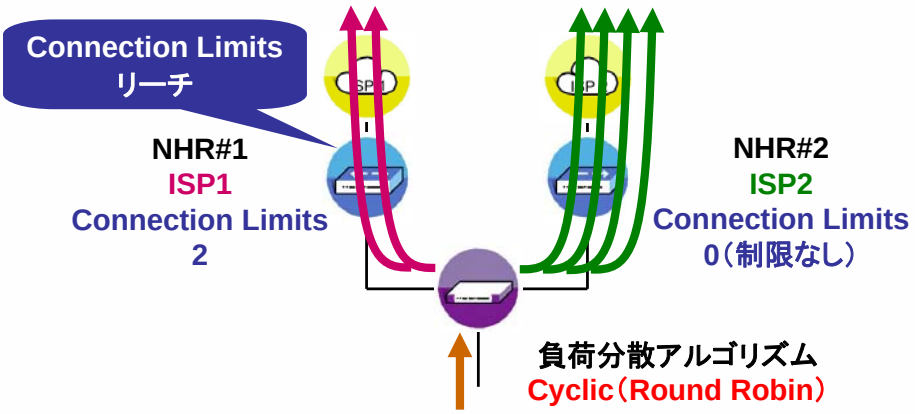
Warm-up Timeの期間中、徐々に振るトラフィックの量を増加し、復旧したNHRに、一気に大量のトラフィックが送信されるのを防ぐ

- NHR Connection Limits
  - NHRに送信するトラフィックの量（コネクション）を制限する機能
  - 処理能力の低いNHRに対して、LinkProofがトラフィックを送信するコネクションの数を制限することができる
  - 制限を越えると、そのNHRにはそれ以上トラフィックを振らない
  - コネクションの数は、クライアントテーブルのエントリ数のこと
    - すなわち、クライアントテーブルがL4モードであれば、

      1コネクション=1セッション

      となります

- NHR Connection Limits

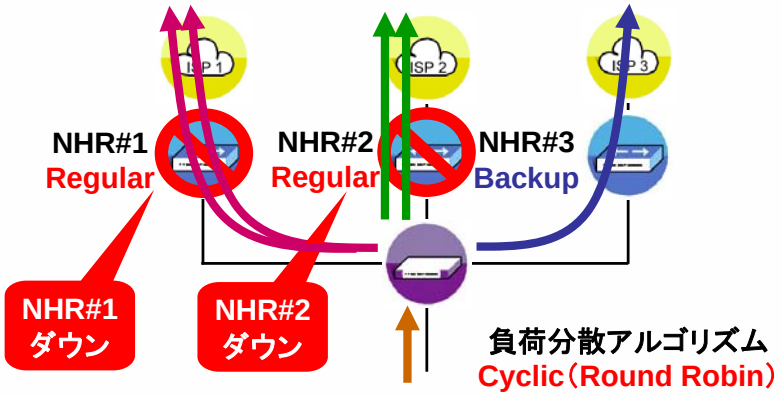


LinkProof # lp next-hop-router table

NHR Address	NHR Name	Operational Status	NHR Priority	Attached Users Number
1.1.1.100	ISP1	active	1	2
2.2.2.200	ISP2	active	1	12

- NHR Operational Mode
  - NHR（ISP回線）をActive・Backupとして設定することが可能
  - ActiveのNHRがすべてダウンしたときに初めて、BackupのNHRにトラフィックが振られる
  - 以下の2つのモードがあります
    - Regular（Active）
      - トラフィックを処理することが出来る
    - Backup
      - Regularに設定されたNHRがすべてダウンした時、トラフィックを処理することが出来る
  - 通常は、Regularモードに設定されたNHRの中から、負荷分散アルゴリズムによって、トラフィックが振られるNHRが決まる

- NHR Operational Mode



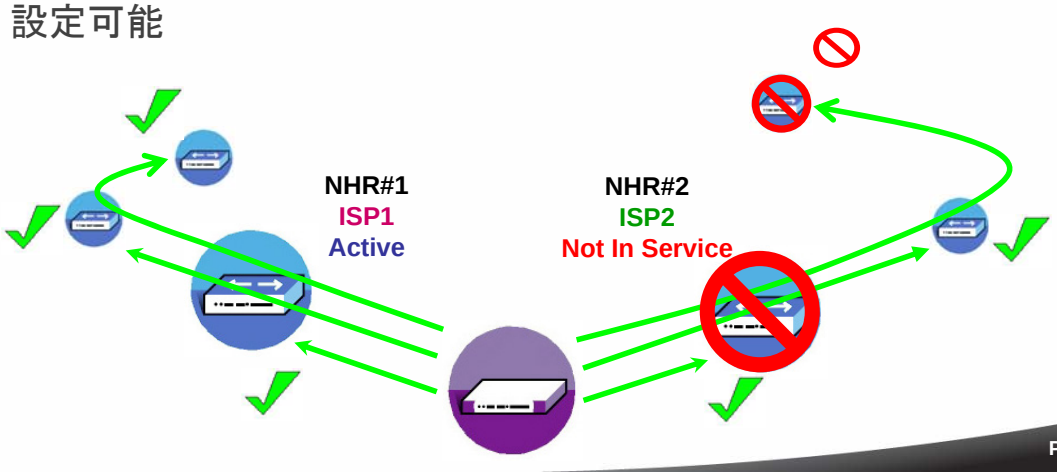
Regularモードに設定されたすべてのNHRがダウンして初めて、BackupモードのNHRにトラフィックが振られる

詳細なヘルスチェック

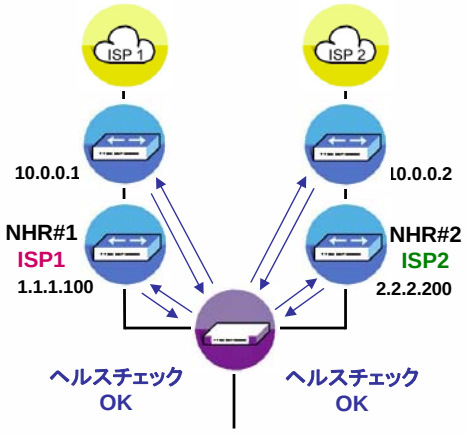
Smart Network. Smart Business.

- NHRを通過して、外部へのヘルスチェックをそのNHRのヘルスチェック結果に反映したい場合に使用する
  - Full Path Health Check
  - Health Monitoring Module

- Full Path Health Check
  - NHRのLinkProof側のインターフェースだけでなく、その先の接続性もチェックするためのもの
  - このPath（道）に沿ったヘルスチェックが失敗したら、該当NHRをダウンとみなします
  - 各NHRで、最大10個のFull Path Health Checkアドレスを設定可能



- Full Path Health Check



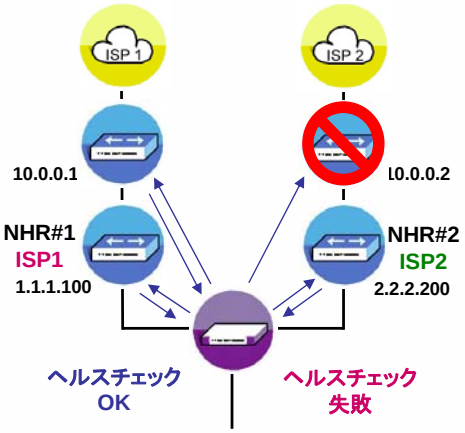
LinkProof #lp global connectivity-check remote-checks-table

NHR IP Address	Check Address	Status
1.1.1.100	1.1.1.100	active
1.1.1.100	10.0.0.1	active
2.2.2.200	2.2.2.200	active
2.2.2.200	10.0.0.2	active

LinkProof # lp next-hop-router table

NHR Address	NHR Name	Operational Status	NHR Priority	Attached Users Number
1.1.1.100	ISP1	active	1	18
2.2.2.200	ISP2	active	1	17

- Full Path Health Check



LinkProof #lp global connectivity-check remote-checks-table

NHR IP Address	Check Address	Status
1.1.1.100	1.1.1.100	active
1.1.1.100	10.0.0.1	active
2.2.2.200	2.2.2.200	active
2.2.2.200	10.0.0.2	notInService

LinkProof # lp next-hop-router table

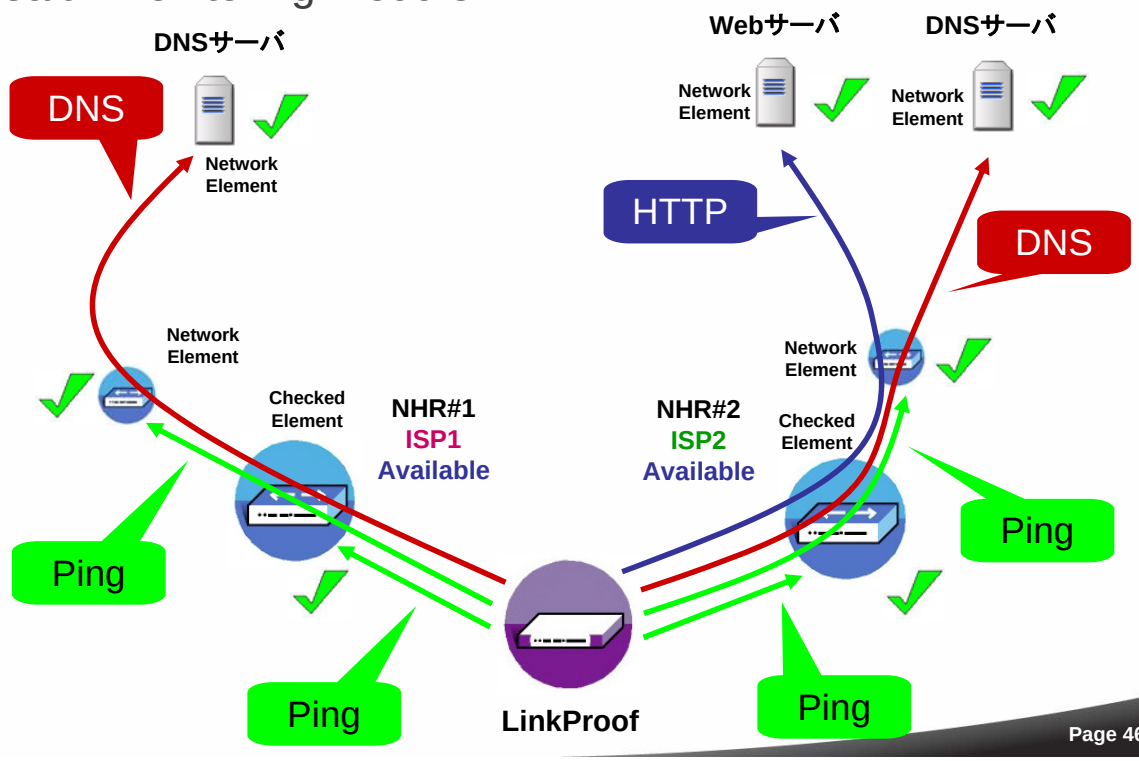
NHR Address	NHR Name	Operational Status	NHR Priority	Attached Users Number
1.1.1.100	ISP1	active	1	30
2.2.2.200	ISP2	notInService	1	0

- Health Monitoring Module
  - Pingだけでなく、多数のプロトコルを使用して、より詳細に外部デバイスに対してヘルスチェックを行い、その結果をNHRのヘルスチェックに反映するもの
  - これは、以下の4つの要素によって成り立っています
    - Network Element
      - ヘルスチェックを実施する対象。外部のデバイス（ISPルータ、外部のWebサーバ等）
    - Checked Element
      - 負荷分散対象のNHR
    - Health Check
      - Network Elementに対して、どのプロトコルを使用して、どれくらいの頻度でヘルスチェックをするのかを決める
    - Health Check Biding
      - Health Checkの結果をChecked Elementに結びつけるもの

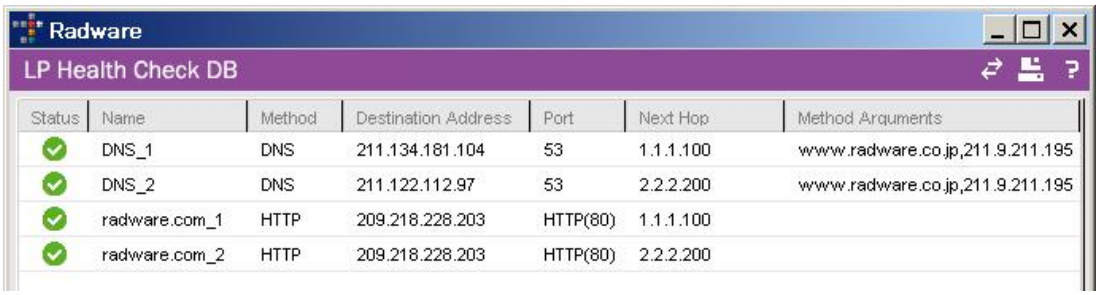
- Health Monitoring Module
  - Health Checkは単体で動作するので、Checked Elementとバインドしないと意味をなさない
  - 1つのChecked Element（NHR）のヘルスチェック結果に、複数のHealth Checkの結果を結びつけることができる
  - その際、Health Check毎にAND・ORを設定することができるため、柔軟なヘルスチェックが可能

radware | 詳細なヘルスチェック
Smart Network. Smart Business.

- Health Monitoring Module



- Health Monitoring Module
  - シナリオ
    - DNS
      - DNSサーバへの名前解決
      - www.radware.co.jp ⇒ 211.9.211.195
    - HTTP
      - Webページへのアクセス
      - 209.218.228.203 (www.radware.com)



Status	Name	Method	Destination Address	Port	Next Hop	Method Arguments
✓	DNS_1	DNS	211.134.181.104	53	1.1.1.100	www.radware.co.jp,211.9.211.195
✓	DNS_2	DNS	211.122.112.97	53	2.2.2.200	www.radware.co.jp,211.9.211.195
✓	radware.com_1	HTTP	209.218.228.203	HTTP(80)	1.1.1.100	
✓	radware.com_2	HTTP	209.218.228.203	HTTP(80)	2.2.2.200	

グルーピング

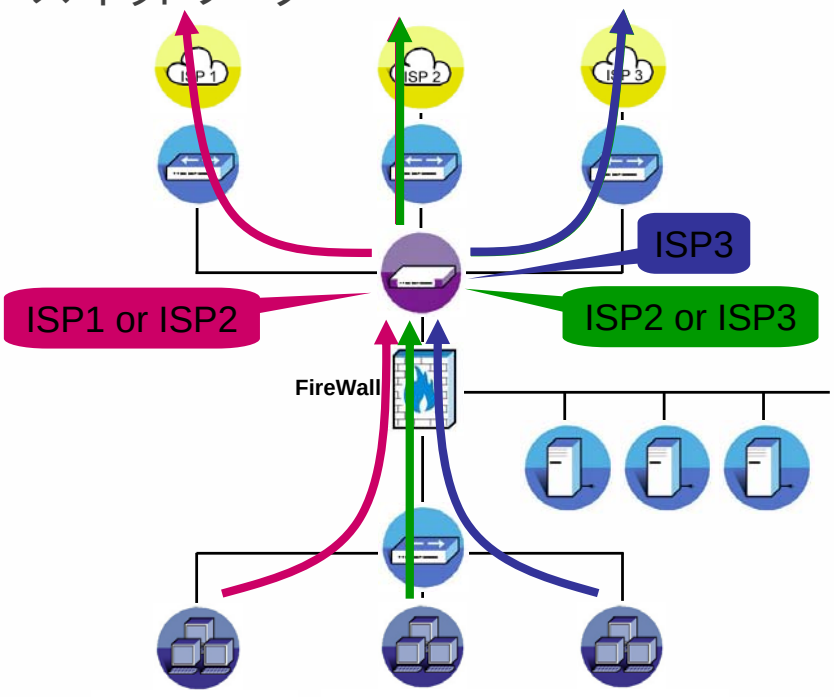
- グルーピング
  - 以下の3つの情報に基づいて、トラフィックを管理者の意図に基づいて、特定のNHR（ISP回線）に送信する機能
    - ソース ネットワーク
      - ソースIPアドレス
    - ディスティネーション ネットワーク
      - ディスティネーションIPアドレス
    - アプリケーション
      - ディスティネーション ポート

※複数のグルーピング設定にマッチするトラフィックが来た場合、優先順位の高い設定が有効になる

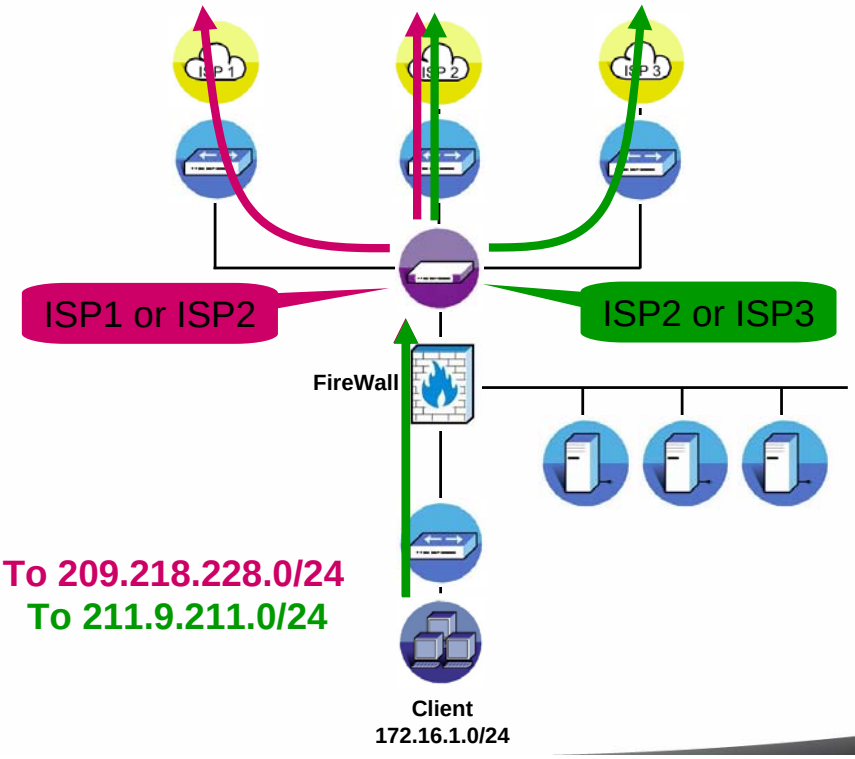
高
- ディスティネーション ネットワーク
- アプリケーション

低
- ソース ネットワーク

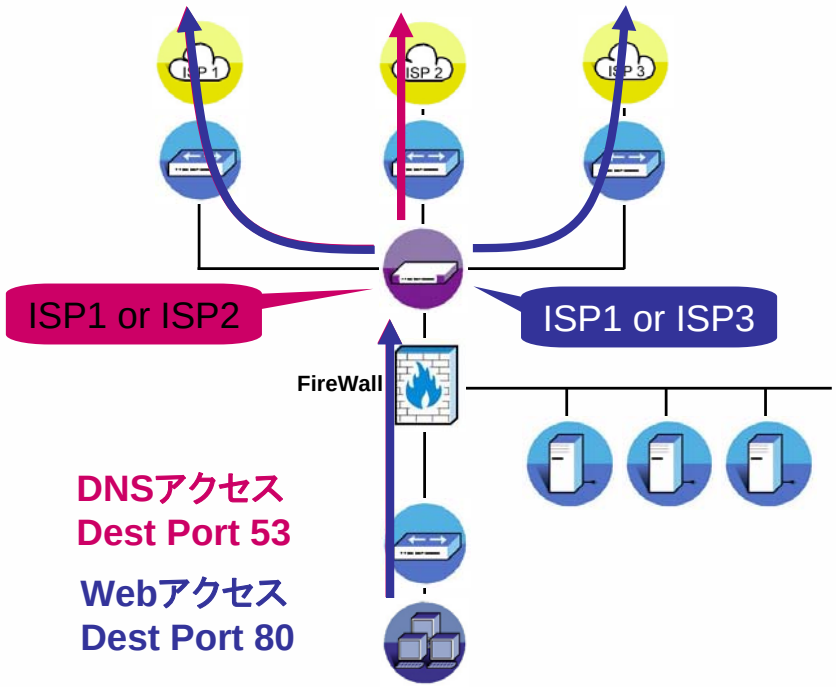
- ソース ネットワーク



• ディスティネーション ネットワーク



• アプリケーション ネットワーク



クライアントテーブル管理

Smart Network. Smart Business.

radware | クライアント テーブル管理

Smart Network. Smart Business.

- クライアント テーブルとは？
  - インバウンド・アウトバウンドのクライアントセッション情報を保存することで、セッションのパーシステンシー（持続性）を維持するためのもの
    - 同一セッションは同じNHR経由で通信させるために使用する
  - Defaultのエイジングタイムは60秒
    - 無通信状態が60秒経過すると、そのエントリは破棄されます

- クライアント テーブルとは？
  - クライアントテーブルには、以下の情報が保存されます
    - セッション情報（IPアドレス、ポート番号）
    - NHR（そのセッションのトラフィックが経由するNHR）
    - NAT（どのNATを使用した通信か T:DN ⇒ ダイナミックNAT）
    - タイムスタンプ（そのセッションが始まった時刻）
    - 方向（Dir:To ⇒ アウトバウンド）

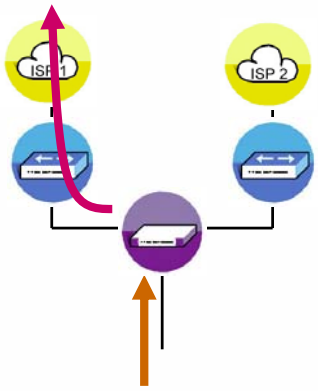
```
LinkProof#lp client table
                    RS CLIENTS Table

Num of Clients : 8
```

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	AttchTime	T	Dir
192.168. 1. 10	65.217.163.224	1. 1. 1.100	1638	80	403	DN	TO
192.168. 1. 10	65.217.163.224	2. 2. 2.200	1637	80	402	DN	TO
192.168. 1. 10	211.134.181.104	2. 2. 2.200	3757	53	396	DN	TO
192.168. 1. 10	65.217.163.224	1. 1. 1.100	1636	80	402	DN	TO
192.168. 1. 10	65.217.163.224	1. 1. 1.100	1634	80	398	DN	TO
192.168. 1. 10	211. 9.211.195	2. 2. 2.200	1635	110	402	DN	TO
192.168. 1. 10	65.217.163.224	1. 1. 1.100	1632	80	396	DN	TO
192.168. 1. 10	65.217.163.224	2. 2. 2.200	1633	80	396	DN	TO

radware | クライアント テーブル管理
Smart Network. Smart Business.

- クライアント テーブルの動作
  - クライアントからのトラフィックがLinkProofに到達したとき、LinkProofはクライアントテーブルにそのセッションのエントリがあるかどうかを調べます
    - エントリがない場合
      - 負荷分散アルゴリズムに基づいて、ロードバランスデシジョンが下されNHRが決定されます。そしてその情報がクライアントテーブルに保存されます
    - エントリがある場合
      - そのエントリに基づいて、同一のNHRに振られます。この場合、新たにロードバランスデシジョンは下されません



LB decision

クライアントテーブルに
エントリがあるかをチェック

ない

負荷分散アルゴリズム
によりNHRを決定

ISP1を使用

ある

エントリと同じ
NHRを使用

クライアントテーブル
エントリ作成

そのNHRのISPから
割り当てられた
アドレスにNAT

クライアントテーブル
エントリ更新

そのNHR経由で
トラフィックを送信

LinkProof#lp client table

RS CLIENTS Table

Num of Clients : 1

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	AttchTime	T	Dir
192.168. 1. 10	65.217.163.224	1. 1. 1.100	1638	80	403	DN	TO

radware | クライアント テーブル管理
Smart Network. Smart Business.

- クライアント テーブル エントリの削除
  - クライアント テーブルのエントリは以下の3つの場合に削除されます
    - トラフィックが振られているNHRがダウンしたとき（Not In Service）
    - クライアントテーブルのエイジング タイム（Default 60秒）を過ぎたとき（無通信状態が60秒以上続いたら削除）
    - “Remove Entry at End of Session” の機能が動作したとき

※“Remove Entry at End of Session”の説明は後述します

- クライアント テーブル モード
  - モードの違いによって、クライアントテーブルに保存する情報や、いつ新たなエントリを作成するのかが変わってきます
  - LinkProofは、以下のクライアントテーブルモードを持っています
    - Layer 3（LinkProofでは使用されないモード）
    - Layer 4
      - Open Entry When Source Port Different
      - Select New NHR When Source Port Different

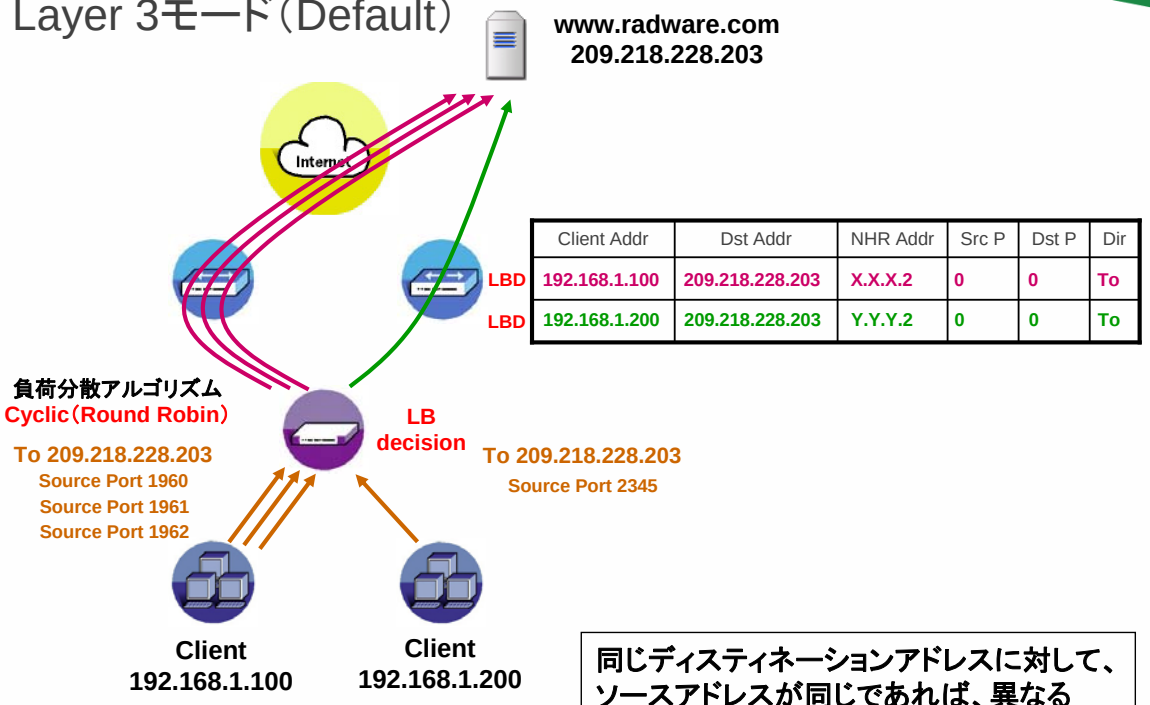
- Layer 3モード（Default）
  - LinkProofでは使用されないモード
  - Layer 3でのパーシステンシーを維持する
  - トラッキングする項目
    - Source IP
    - Destination IP
  - このモードでは、同じSource IPから同じDestination IPにおいてすべてのセッションは1つのエントリに集約され、同じNHRに振られます

```
LinkProof#lp client table
                                RS CLIENTS Table

Num of Clients : 2
```

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	AttchTime	T	Dir
192.168. 1. 10	211.134.181.104	2. 2. 2.200	0	0	4216		TO
192.168. 1. 10	209.218.228.203	1. 1. 1.100	0	0	4217		TO

- Layer 3モード（Default）



Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
192.168.1.100	209.218.228.203	X.X.X.2	0	0	To
192.168.1.200	209.218.228.203	Y.Y.Y.2	0	0	To

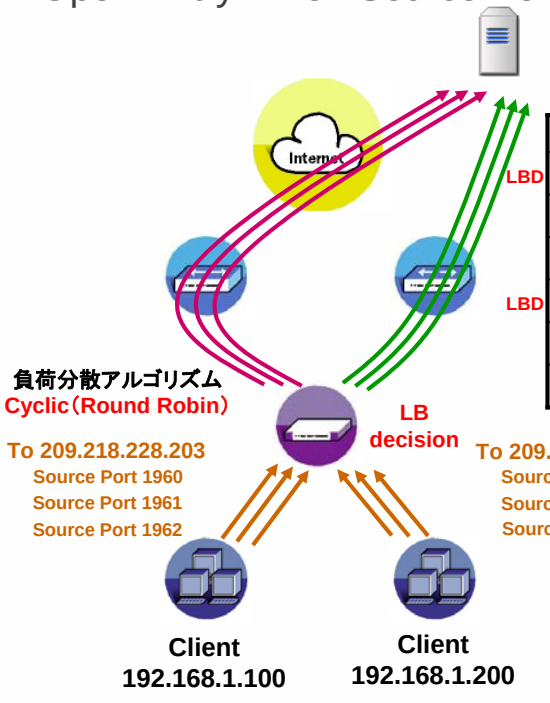
同じディスティネーションアドレスに対して、ソースアドレスが同じであれば、異なるソースポートでも、同じNHRを選択する

- Layer 4モード
  - Layer 4でのパーシステンシーを維持する
  - トラッキングする項目
    - Source IP / Destination IP
    - Source Port / Destination Port
  - Layer 4モードはさらに以下の2つに分けられます
    - Open Entry When Source Port Different
    - Select New NHR When Source Port Different

- Layer 4モード
  - Open Entry When Source Port Different
    - 動作はLayer 3モードと同じだが、ソースポート毎にエントリを作成する
      - ソースポート毎にエントリを作成
      - しかしながら、ソースIP毎にNHRが決められる

radware | クライアント テーブル管理
Smart Network. Smart Business.

- Layer 4モード
  - Open Entry When Source Port Different



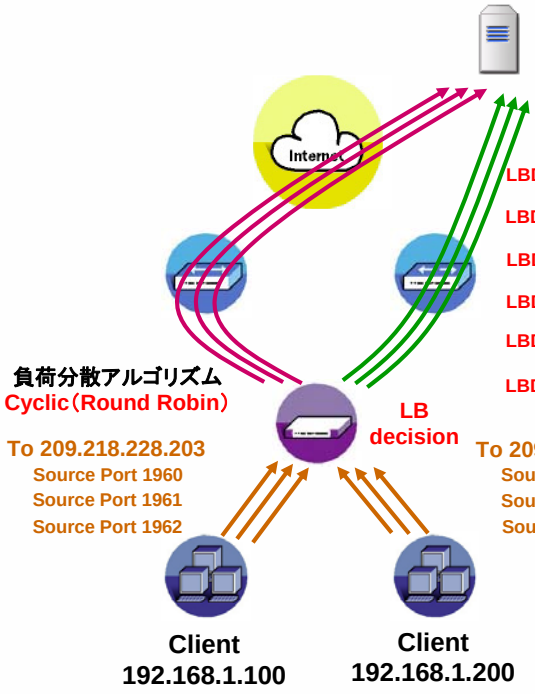
	Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
LBD	192.168.1.100	209.218.228.203	X.X.X.2	1960	80	To
	192.168.1.100	209.218.228.203	X.X.X.2	1961	80	To
	192.168.1.100	209.218.228.203	X.X.X.2	1962	80	To
LBD	192.168.1.200	209.218.228.203	Y.Y.Y.2	2345	80	To
	192.168.1.200	209.218.228.203	Y.Y.Y.2	2346	80	To
	192.168.1.200	209.218.228.203	Y.Y.Y.2	2347	80	To

同じディスティネーションアドレスに対して、ソースアドレスが同じでもソースポート毎にエントリを作成するが、同じNHRを選択する

- Layer 4モード
  - Open Entry When Source Port Differentのオプション
    - Remove Entry at End of Session
      - クライアントテーブルのエイジングタイムが切れる前に、不必要なエントリを削除する機能
      - TCPセッションについてのみ有効
        - » TCPセッションがクローズした時に、エントリを削除します（FIN、RSTを監視することでセッションクローズを検知）
      - これを使用することにより、クライアントテーブルのエントリは、すべて通信継続中のもののみとなり、クローズしたTCPセッションのエントリはすぐに削除されるため、メモリリソースの消費を抑え、メモリ利用率を低下させることが出来ます

- Layer 4モード
  - Select New NHR When Source Port Different
    - ソースポート毎に新たなエントリを作成
    - ソースポート毎にLB decisionが行われる
      - セッション毎にLB decisionが行われる

- Layer 4モード
  - Select New NHR When Source Port Different



	Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
LBD	192.168.1.100	209.218.228.203	X.X.X.2	1960	80	To
LBD	192.168.1.100	209.218.228.203	Y.Y.Y.2	1961	80	To
LBD	192.168.1.100	209.218.228.203	X.X.X.2	1962	80	To
LBD	192.168.1.200	209.218.228.203	Y.Y.Y.2	2345	80	To
LBD	192.168.1.200	209.218.228.203	X.X.X.2	2346	80	To
LBD	192.168.1.200	209.218.228.203	Y.Y.Y.2	2347	80	To

同じディスティネーションアドレスに対して、ソースアドレスが同じでもソースポート毎にエントリを作成し、異なるNHRを選択する

- アプリケーション毎のエイジングタイム
  - クライアントテーブルのエイジングタイムは、アプリケーション毎に変更することができます
  - 無通信状態が続いてもエントリを削除せず、パーシステンシーを長時間維持したい場合に使用します
  - 例
    - LinkProof を経由してTelnetをしている状態で、無通信状態が長時間続いたあとも、継続してアクセスできるようにしたい

```
LinkProof#lp global client-table application-aging-time get
        Aging By Application Port
```

Application Port	Aging Time
23	3600

- どちらのクライアントテーブルモードを選択すべきか？
  - Open Entry When Source Port Different
  - Select New NHR When Source Port Different
- 例
  - シナリオ
  - 社内のユーザがプロキシを経由して、Webブラウジィングを しいている環境の場合
    - LinkProofに到達するソースアドレスは、プロキシのアドレスになる
      - Open Entry When Source Port Differentを使用すると、プロキシ経由のトラフィックは、同一の宛先に対して、同一のNHRを選択してしまう

      - ロードバランス結果に偏りがでてしまう可能性がある

      - Select New NHR When Source Port Different

冗長化

radware | LinkProofの冗長化

Smart Network. Smart Business.

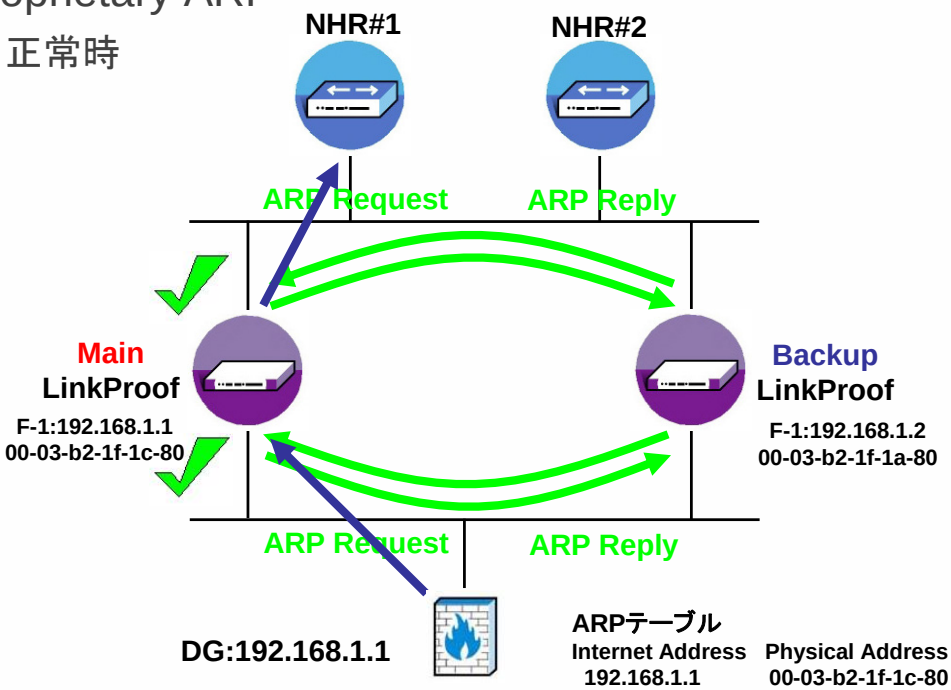
- LinkProofは以下の2つの冗長構成をサポートします
  - Proprietary ARP
  - VRRP（推奨）
- 冗長構成時におけるセッションパーシステンシー
  - クライアントテーブル エントリのミラーリング

radware | LinkProofの冗長化 - ARP

Smart Network. Smart Business.

- Proprietary ARP
  - ARPを使用したヘルスチェックを用いた冗長構成
    - BackupデバイスがMainデバイスのインターフェースにARPリクエストを送信する。ARPリプライが返ってきたら、そのインターフェースはUpしていると判断する
    - ARPリプライが来ないと、Backupデバイスは、Mainデバイスがダウンしていると判断する。そしてネットワーク上のホストのARPテーブルを更新するためにGratuitous ARPを送信し、MainデバイスのIPアドレスをBackupデバイスが引き継ぐ

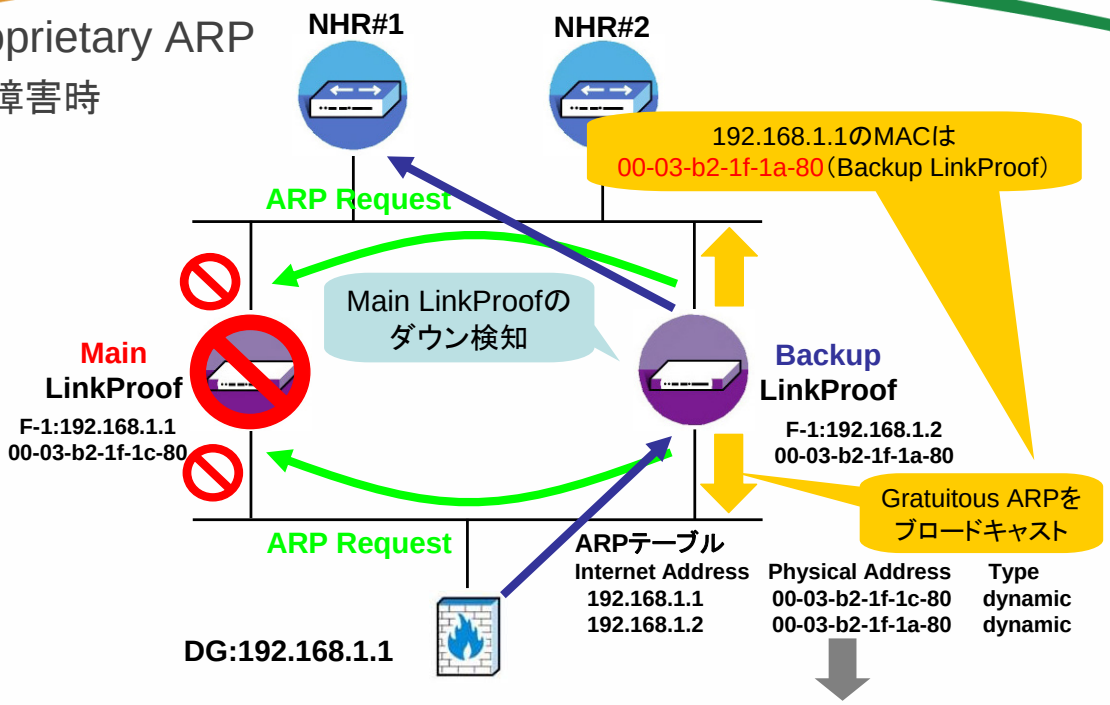
- Proprietary ARP
  - 正常時



ARPテーブル

Internet Address	Physical Address	Type
192.168.1.1	00-03-b2-1f-1c-80	dynamic
192.168.1.2	00-03-b2-1f-1a-80	dynamic

- Proprietary ARP
  - 障害時



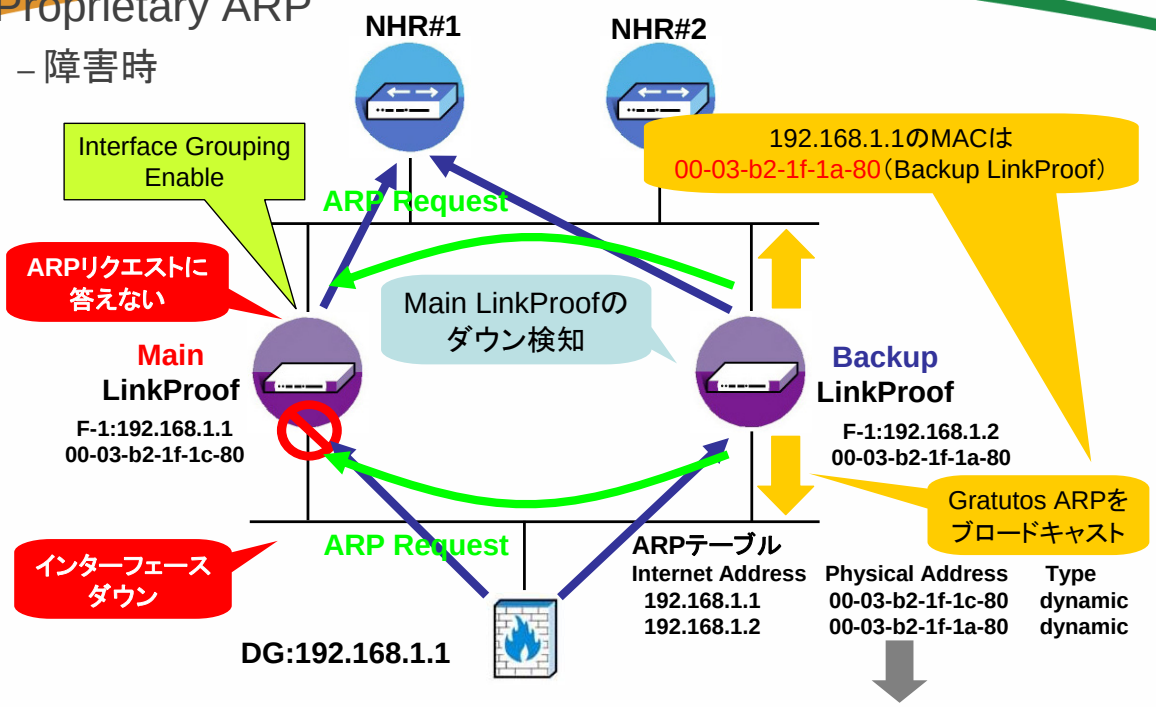
ARPテーブル

Internet Address	Physical Address	Type
192.168.1.1	00-03-b2-1f-1c-80	dynamic
192.168.1.2	00-03-b2-1f-1a-80	dynamic

Internet Address	Physical Address	Type
192.168.1.1	00-03-b2-1f-1a-80	dynamic
192.168.1.2	00-03-b2-1f-1a-80	dynamic

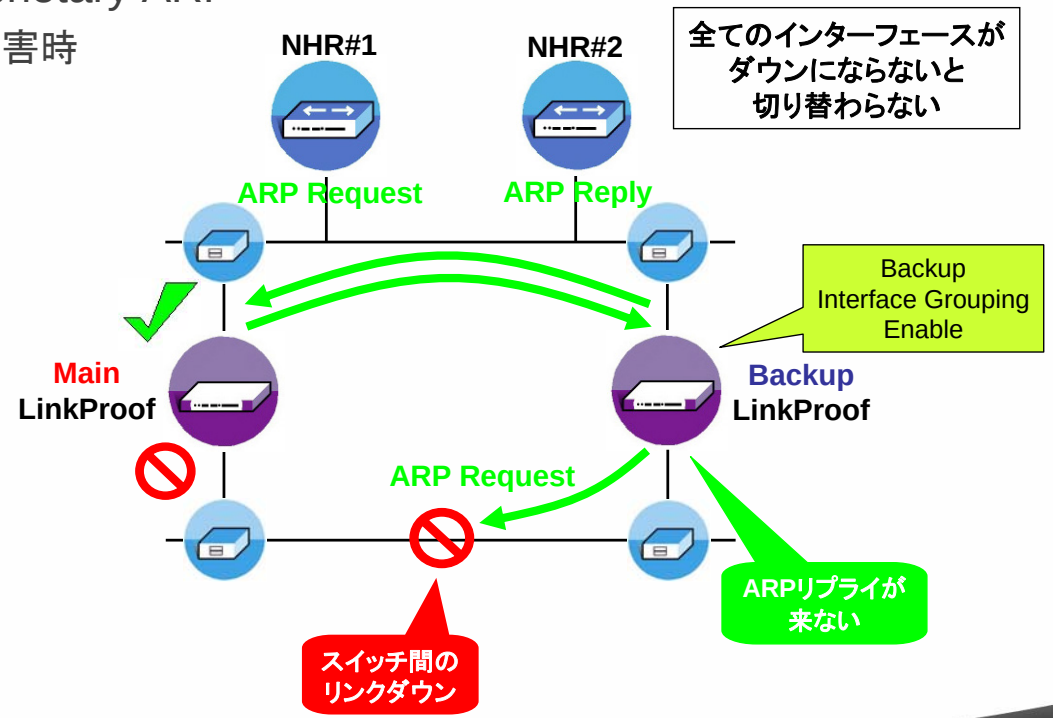
- Proprietary ARPのパラメータ
  - Interface Grouping（MainデバイスでEnable）
    - Mainデバイスの1つのインターフェースが落ちると、他のすべてのインターフェースでのARPリクエストに対する応答をしない
    - これによってBackupデバイスは、Mainデバイス全体のダウンと判断し、切り替わる

- Proprietary ARP
  - 障害時



- Backup Interface Grouping（BackupデバイスでEnable）
  - Mainデバイスのすべてのインターフェースへのヘルスチェックが失敗したときに切り替わりる。冗長LPが冗長のスイッチに接続している場合に有効である
  - もしスイッチ間の接続がフェイルしても、Mainデバイスは依然としてActiveのまま動作する

- Proprietary ARP
  - 障害時

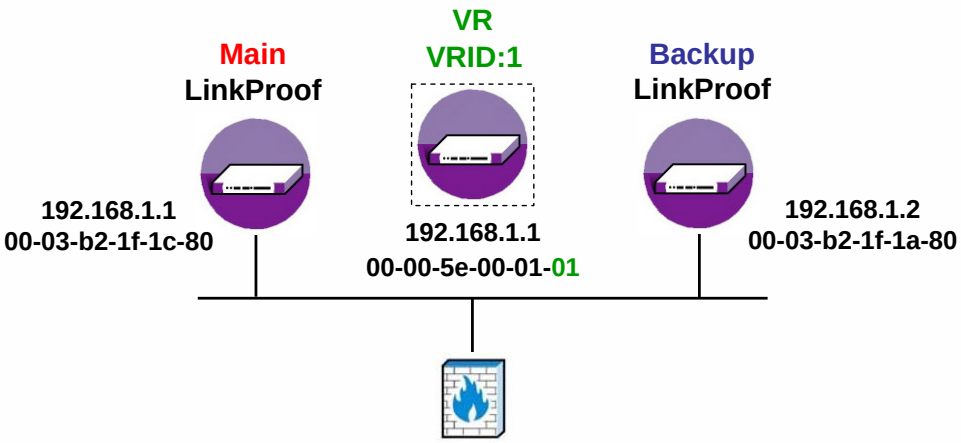


- Proprietary ARPのパラメータ
  - Interface GroupingとBackup Interface Groupingの設定の意図
    - どのような場合に切り替わるのかを、設定によって変更したい
  - Default設定における両デバイスの動作意図
    - Mainデバイスの動作意図
      - 自分に何かの障害があった場合には、すぐに切り替わってほしい
        - » 1つのインターフェースがダウンしたら、すべてのインターフェース がダウンしたようにみせる
    - Backupデバイスの動作意図
      - Mainデバイスが完全にダウンした場合に、切り替わる
        - » MainデバイスへのARPによるヘルスチェックが、すべての インターフェースにおいて失敗したときにのみ、切り替わる

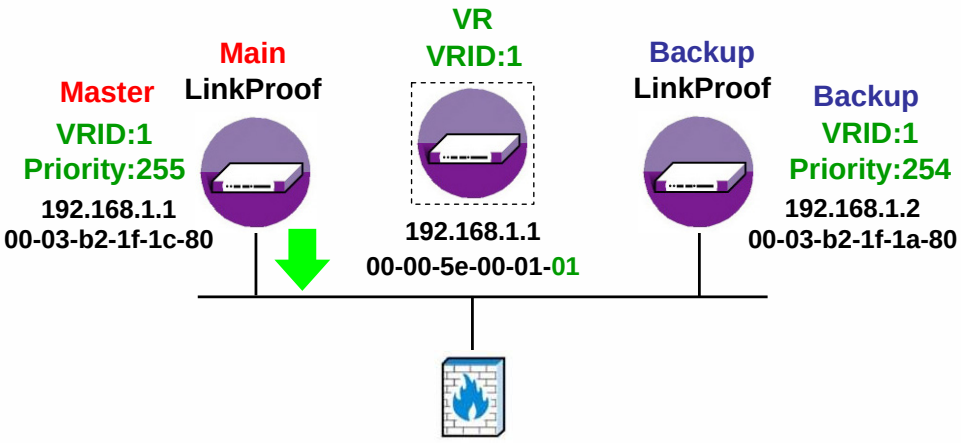
radware | LinkProofの冗長化 - ARP
Smart Network. Smart Business.

- Proprietary ARPのパラメータ
  - Backup Fake ARP（BackupデバイスでEnable）
    - Mainデバイスが復旧したときに、Backupデバイスが引き継いだIPアドレスが、またMainデバイスに戻ったというGratutousARPを、Backupデバイスが投げることで、切り戻しの時間を短縮するもの
    - これによってホストのARPテーブルを書き換え、Mainデバイスへの切り戻しをより高速に行うことができる

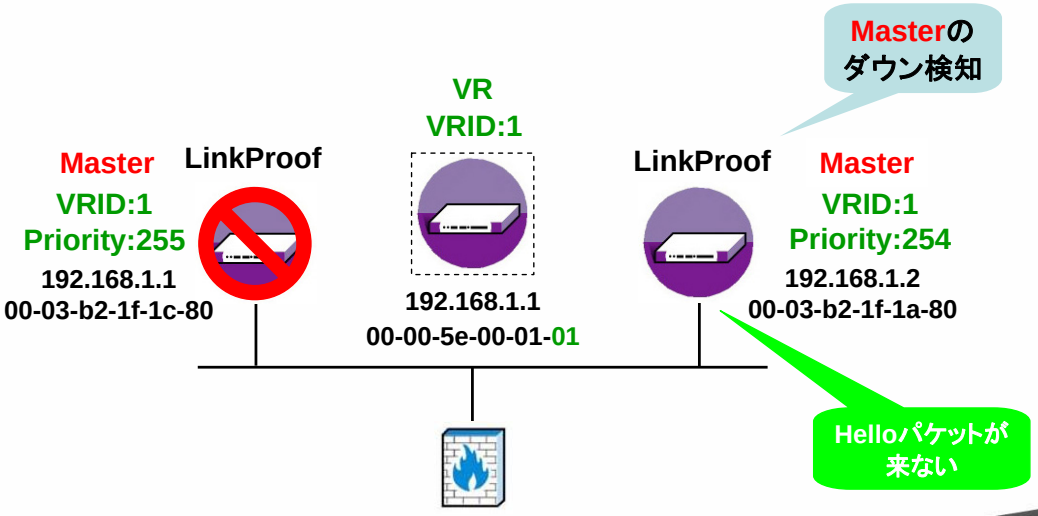
- VRRPの基本コンセプト
  - VR（Virtual Router：仮想ルータ）
  - VRには、VRIDを付加し、それと関連付けるIPアドレスを設定する（このアドレスに対して冗長化が提供される）
  - VRには、自動的にVRMACが付加される



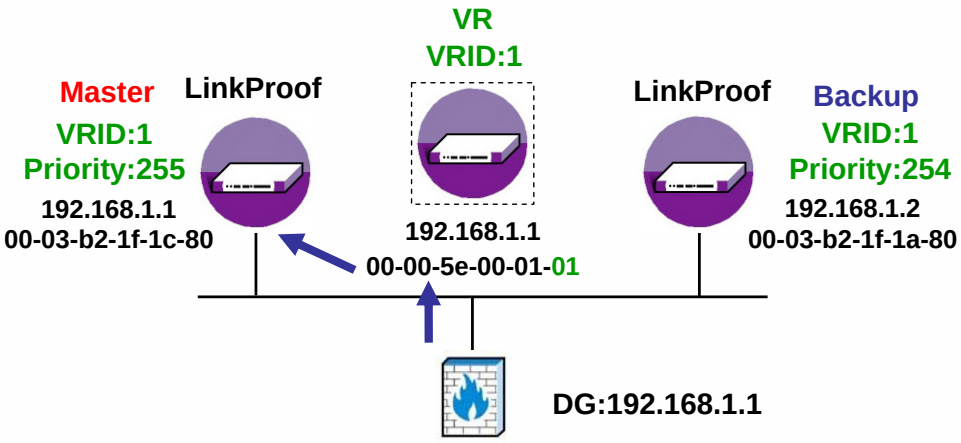
- VRのプライオリティ（優先度）
  - 各々のデバイスで、VRに異なるプライオリティを設定
  - 最もプライオリティが高いデバイスが、そのVRのMasterになる
  - VRのMasterデバイスは、自分がUpしていることを示すために、他のデバイスに常にHelloパケットを送る



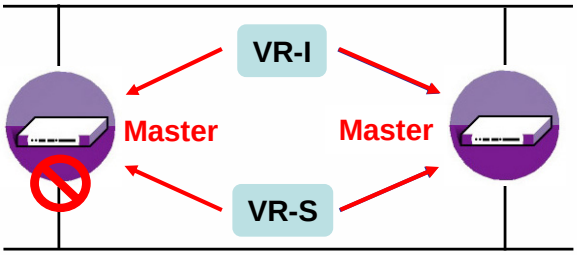
– Backupデバイスは、そのHelloパケットが受信できなくなると、そのVRのMasterがダウンしたと見なします
– Masterがダウンしたら、次にプライオリティの高いデバイスがMasterになります



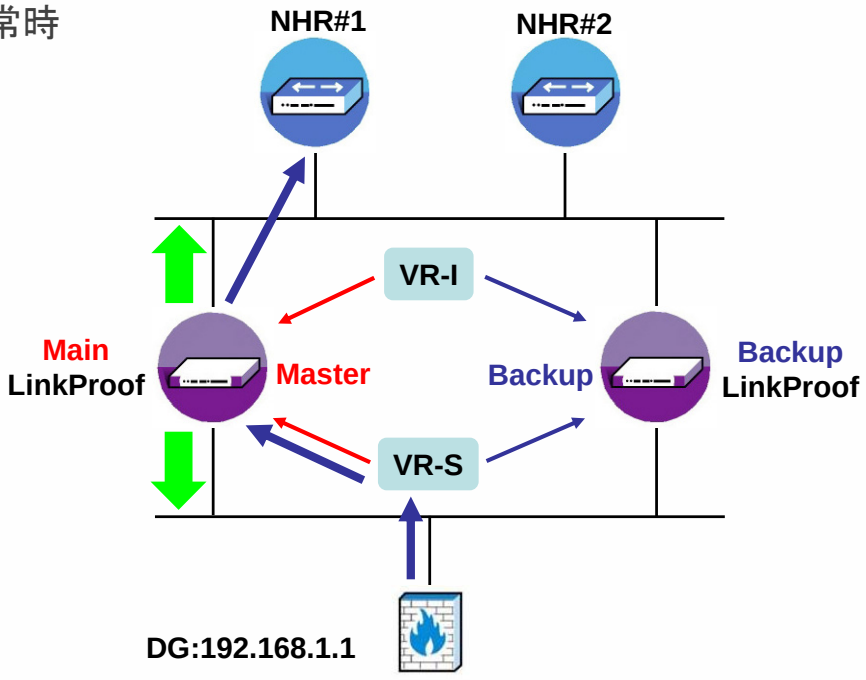
• 冗長化したIPアドレスに対するトラフィックの処理
– LinkProof手前のルータは、Gatewayとして、VRに関連付けたIPアドレスを指定します（DG:192.168.1.1）
– このアドレスのMACは、VRMACになります
– MasterのデバイスがVRMAC宛のトラフィックを処理します



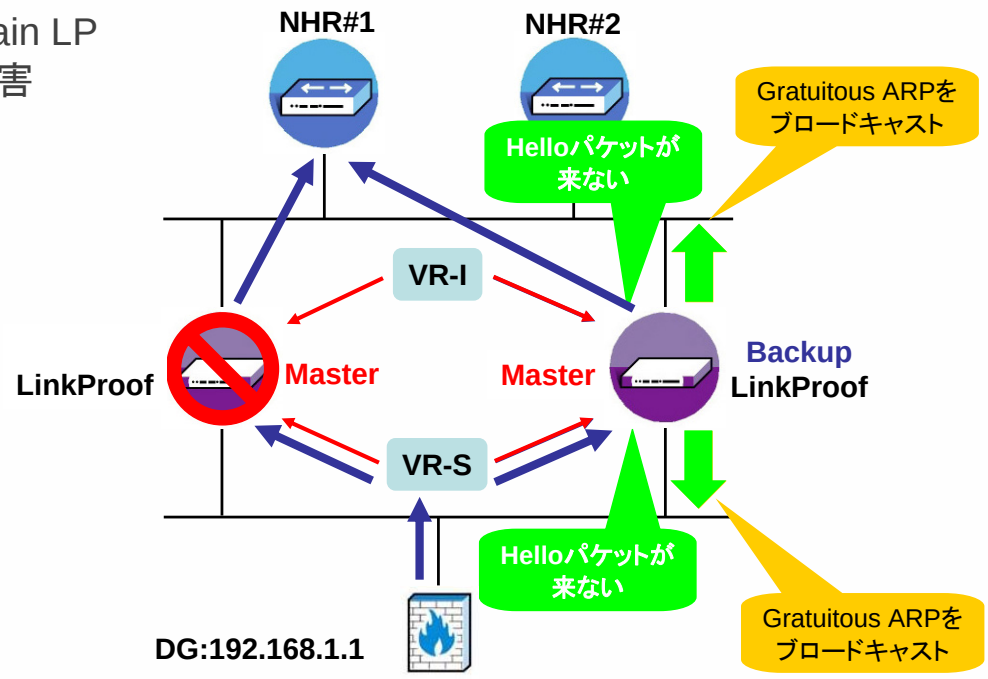
- VRRPの構成
  - LinkProofの標準的な構成では、VRはインターネット側とサーバ側（内部ネットワーク側）の2つ作成します
    - VR-I
      - インターネット側
    - VR-S
      - サーバ側（内部ネットワーク側）
  - Defaultパラメータによる切り替わり動作
    - 障害時において上記2つのVRが同時に切り替わります



- VRRP
  - 正常時



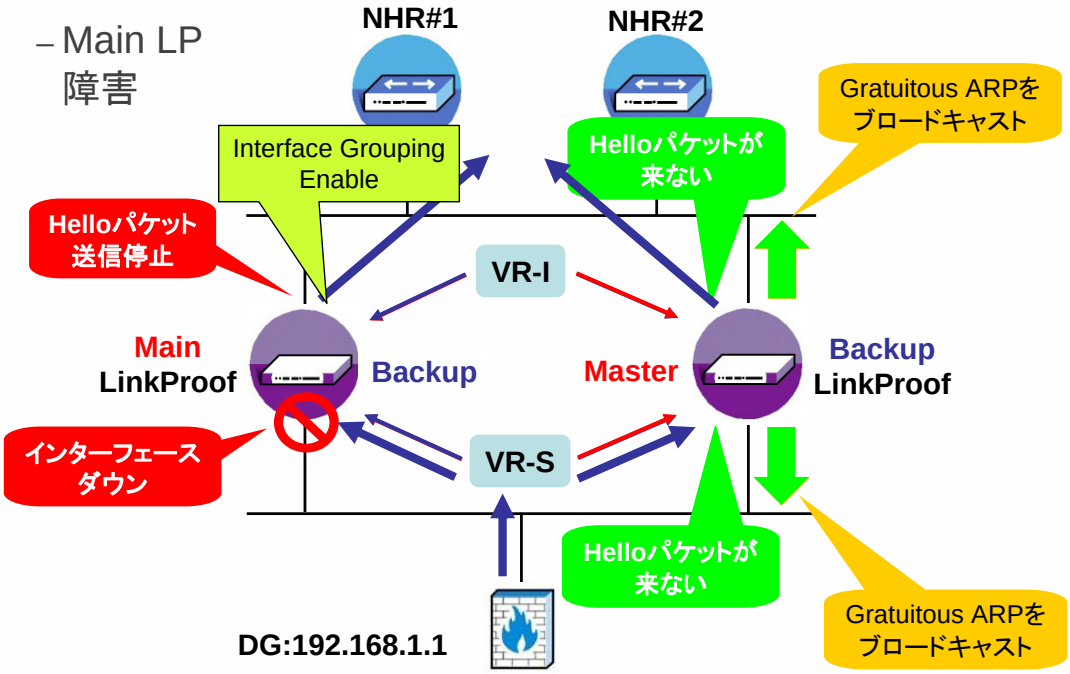
- VRRP
  - Main LP 障害



- VR（仮想ルータ）のパラメータ
  - LinkProofがVRRPの動作において、VR毎の切り替わりではなく すべてのVR毎（デバイス毎）の切り替わりをするためには、 以下のパラメータが関連します
    - Interface Grouping
    - Backup Interface Grouping

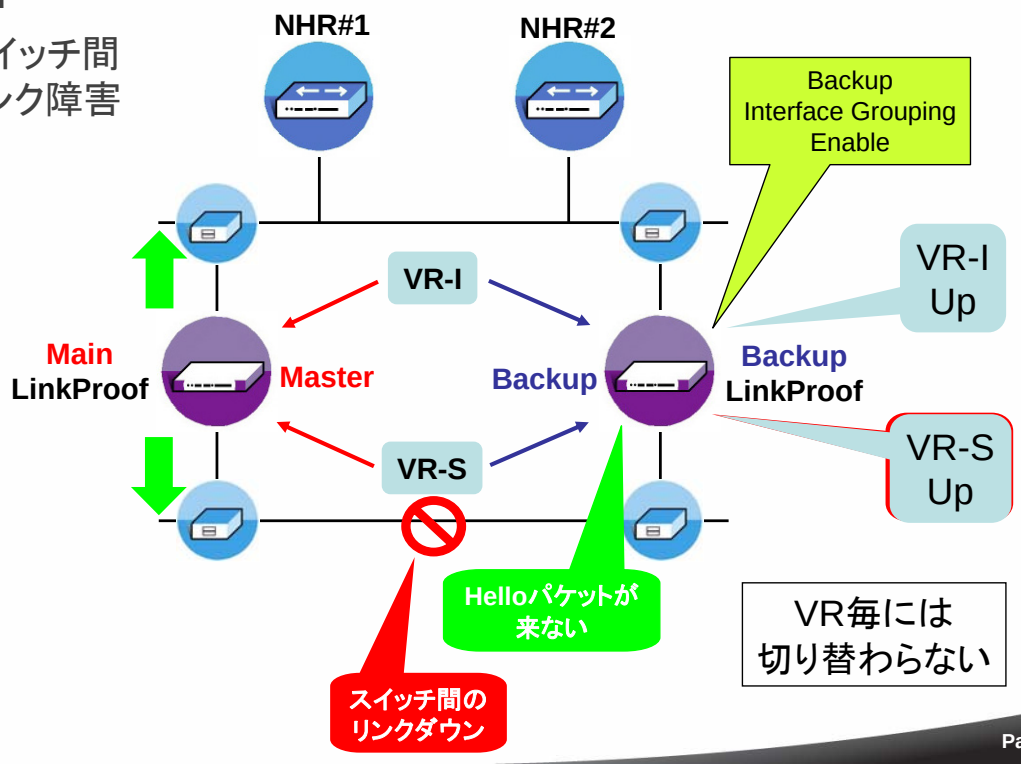
- VR（仮想ルータ）のパラメータ
  - Interface Grouping（MainデバイスでEnable）
    - VRの1つのインターフェースがダウンすると、他のVRのインターフェースからのHelloパケットの送信も止める
    - Backupデバイスに対して、Mainデバイスのすべての VRがダウンしたように見せる

- VRRP
  - Main LP 障害



- VR（仮想ルータ）のパラメータ
  - Backup Interface Grouping（BackupデバイスでEnable）
    - 全てのVRのHelloが来なくなったら、VRのステータスをBackupからMasterにステータスを変える
    - 複数VRがあり、1つのVRだけHelloが来ない場合は、切り替わらない

- VRRP
  - スイッチ間リンク障害

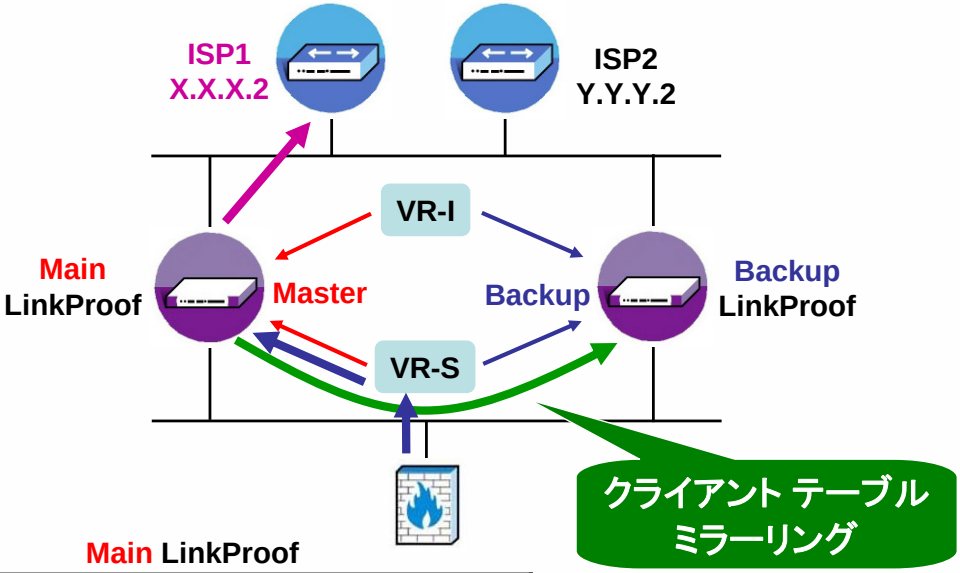


- VR（仮想ルータ）のパラメータ
  - Interface GroupingとBackup Interface Groupingの設定の意図
    - どのような場合に切り替わるのかを、設定によって変更したい
  - Default設定における両デバイスの動作意図
    - Mainデバイスの動作意図
      - 自分に何かの障害があった場合には、すぐに切り替わってほしい
        - » 1つのインターフェースがダウンしたら、すべてのインターフェースがダウンしたようにみせる（Helloパケットの送信を止める）
    - Backupデバイスの動作意図
      - すべてのVRがダウンした場合に、切り替わる
        - » Mainデバイスから、すべてのVRのハローが来なくなったときのみ、切り替わる

- VR（仮想ルータ）のパラメータ
  - Preemption
    - Mainデバイスに障害が発生すると、Backupデバイスはすべての VRのマスタを引き継ぎます
    - その後、Mainデバイスが復旧した際、即座にMainデバイスに Masterが移るか、もしくは復旧してもBackupにとどまるかの設定
      - True
        - » 復旧したMainデバイスが、即座にVRのMasterになる
      - False
        - » 復旧したMainデバイスが、VRのBackupにとどまる

- クライアントテーブル エントリのミラーリング
  - 冗長化の切り替わり後も、セッションのパーシステンシーを維持するための機能
  - Mainデバイスの障害による切り替わりに備えて、Mainデバイスのクライアントテーブル エントリをBackupデバイスにコピーします
    - ミラーリングの動作
      - 10秒おきに、MainデバイスからBackupデバイスに、クライアントテーブルの新規エントリをコピーする。
      - プロトコルはUDP, Source Port:2092, Destination Port:2092を使用
      - エントリが、1パケットに収まらない場合は、複数パケットを送信
      - Mainデバイスのエントリが消えた時には、Backupデバイスに通知し、Backupデバイスのエントリも削除
      - エントリの削除通知をする前に、Mainデバイスがダウンしてしまった場合、Backupデバイスのエントリのエイジングは、Backupデバイスのクライアントテーブルのエイジングタイムに準じます

- クライアントテーブルミラーリング



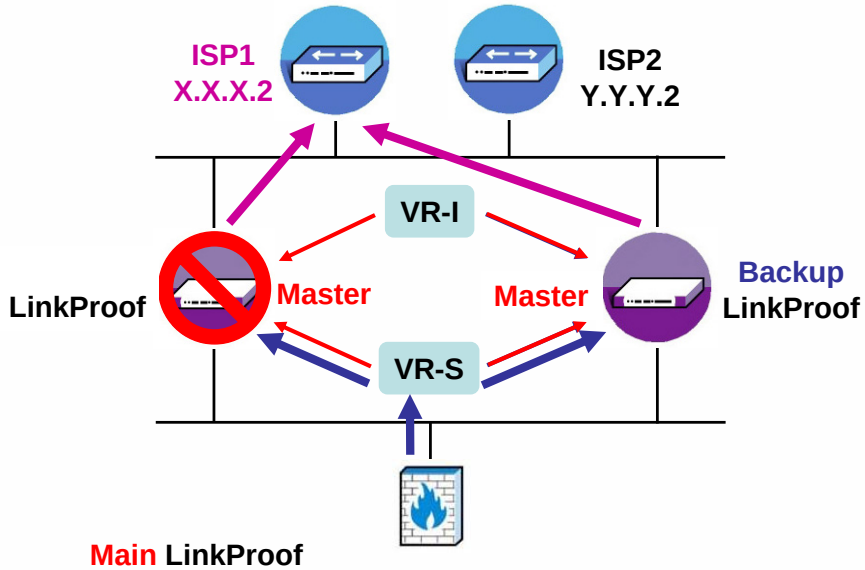
Main LinkProof

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
192.168.1.100	209.218.228.203	X.X.X.2	1661	80	To

Backup LinkProof

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
192.168.1.100	209.218.228.203	X.X.X.2	1661	80	M

- クライアントテーブルミラーリング



Main LinkProof

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
192.168.1.100	209.218.228.203	X.X.X.2	1661	80	To

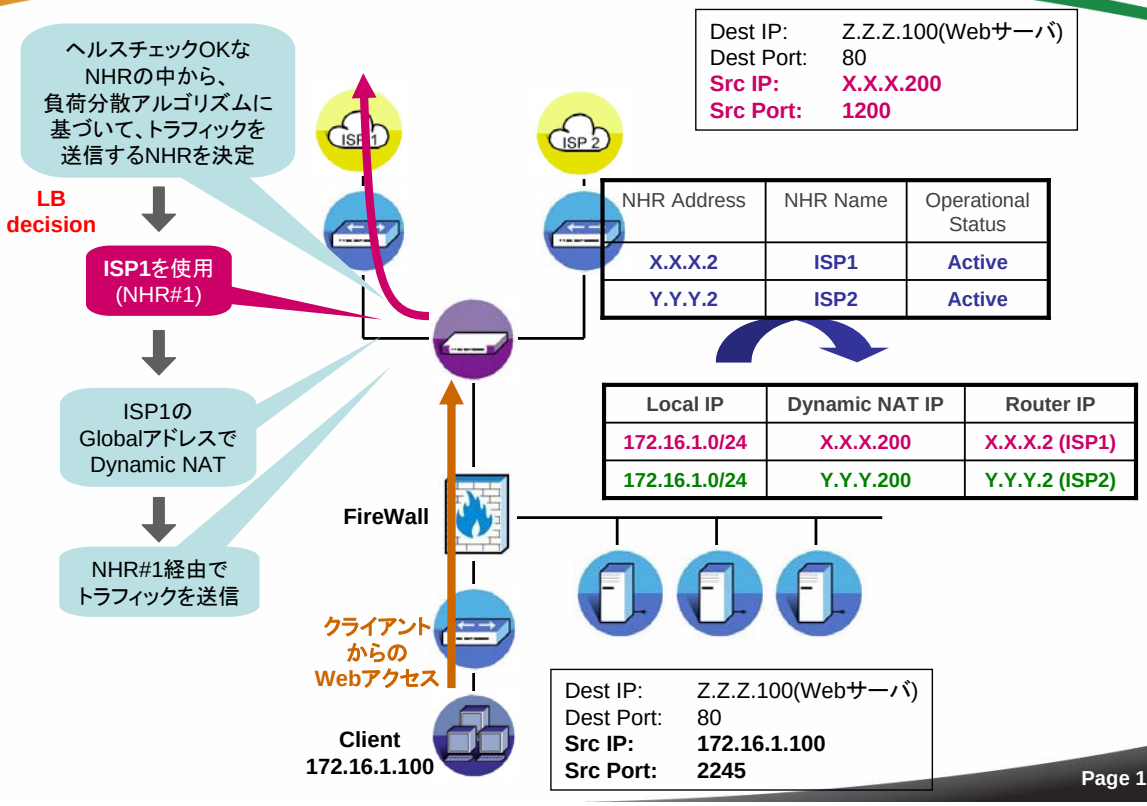
Backup LinkProof

Client Addr	Dst Addr	NHR Addr	Src P	Dst P	Dir
192.168.1.100	209.218.228.203	X.X.X.2	1661	80	M

近接性（Proximity）

- 近接性とは？
  - 通信相手に対して、どちらの回線を利用した方が、ネットワーク的により近いのかを動的に判断する機能
  - 近接性を確認するために、通信相手に対して近接性チェック（Proximityチェック）を行います
  - 近接性チェックは、実際の環境で行うので、ラウンドロビンやリースト コネクションなどでは計れない、実際インターネットのネットワークの状況を元に、通信相手に対して、より効率的な回線を選択することができます
  - LinkProofは、近接性を遅延時間やホップ数を元に計算します
  - 近接性は動的に計測することも、静的に設定することも可能です

- アウトバウンド トラフィックの制御
  - アウトバウンド トラフィック（内部から外部へのトラフィック）を近接性チェックを使用して、制御する
  - アウトバウンド近接性チェックの動作
    - ある宛先ホストに対しての、初めの通信は、通常のLB decisionを元に行われます
    - その後、その宛先ホストに対して、近接性チェックを行います
    - 近接性チェックの結果は、/24でProximityテーブルに保存されます
    - 以降、同一の宛先（/24）への通信は、近接性チェックの結果を元に、最も効率的な回線を使用して、通信をすることができます

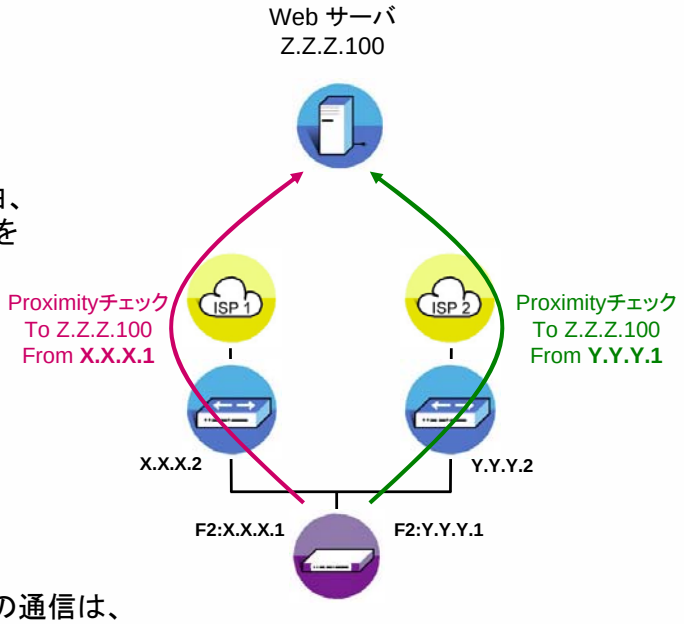


宛先サーバに対して、
Proximityチェックを行う

Proximityチェックは、ISP1経由、
ISP2経由供に行い、その結果を
Proximityテーブルに/24の
ネットワークで載せる

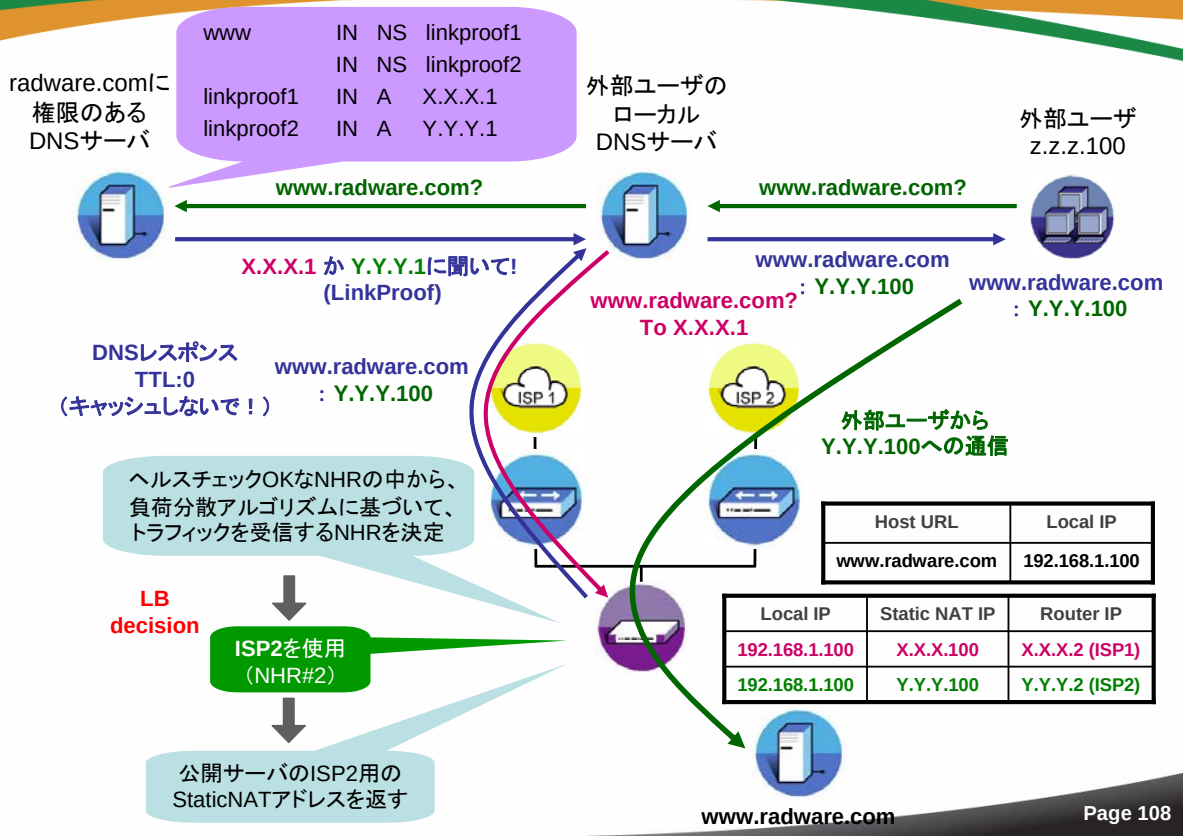
Dynamic proximity table

Subnet Server	Latency	Hops
Z . Z . Z . 0		
Hits counter 0		
Y. Y. Y. 2	13	102
X. X. X. 2	17	224



以後、同一サブネットに対しての通信は、
この結果を元に、使用するISPを選択する

- インバウンド トラフィックの制御
  - インバウンド トラフィック（外部から内部へのトラフィック）を近接性チェックを使用して、制御する
  - LinkProofをDNSサーバとして設定し、外部からアクセスして欲しいISP回線のアドレスで、DNSレスポンスを返すことにより、インバウンドトラフィックを制御する
  - インバウンド近接性チェックの動作
    - 内部ホストに対してのDNSクエリに対して、そのStatic NATアドレスを返す
    - DNSクエリをしてきたホストに対して、近接性チェックを行う
    - 近接性チェックの結果は、/24でProximityテーブルに保存されます
    - 以降、同一の送信元（/24）からのDNSクエリに対しては、近接性チェックの結果を元に、最も効率的な回線を使用したStatic NATアドレスを返答します



近接性

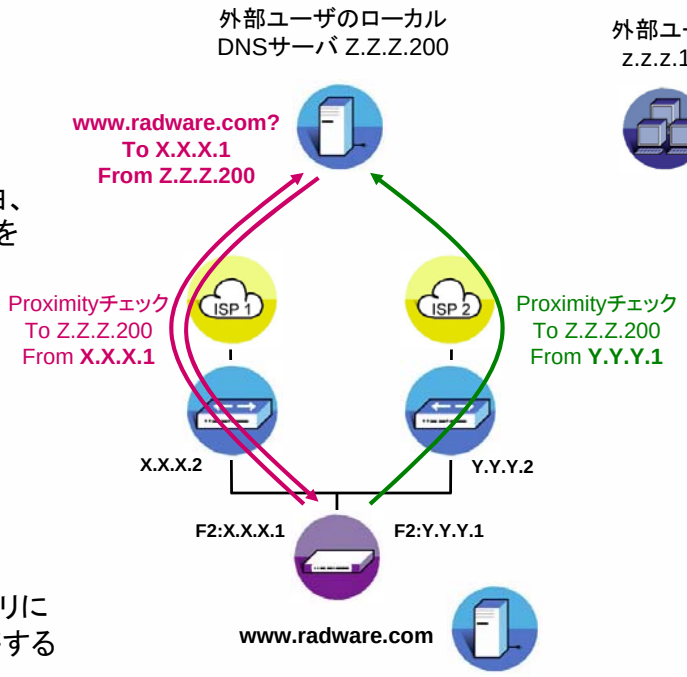
Smart Network. Smart Business.

LinkProofは、DNSクエリを
送信したサーバに対して、
Proximityチェックを行う

Proximityチェックは、ISP1経由、
ISP2経由供に行い、その結果を
Proximityテーブルに/24の
ネットワークで載せる

Dynamic proximity table		
Subnet Server	Latency	Hops
Z . Z . Z . 0 Hits counter 0		
Y. Y. Y. 2	10	124
X. X. X. 2	15	204

同一サブネットからのDNSクエリに
対しては、この結果を元に返答する

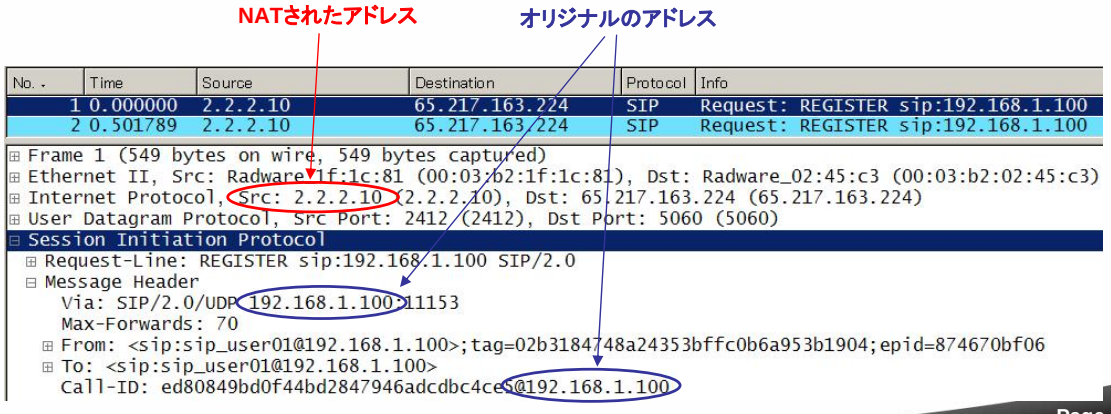


仮想トンネル(Virtual Tunneling)

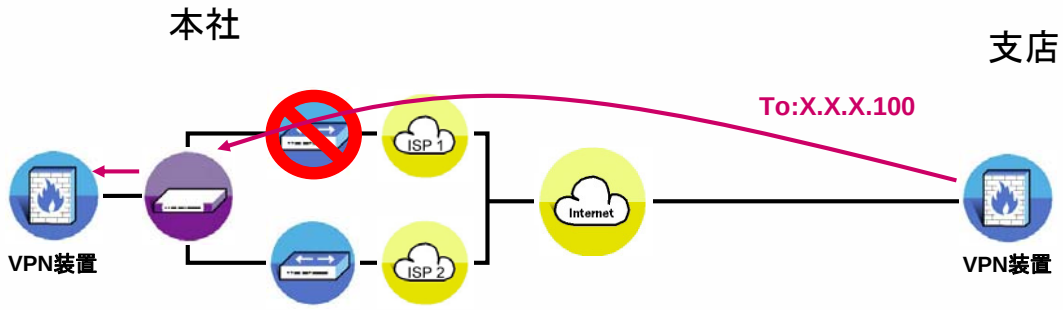
Smart Network. Smart Business.

- 仮想トンネルとは？
  - NATデバイス越えが困難なアプリケーション（SIP等）に対しても、回線負荷分散の構成を提供するための機能
    - ソースアドレスがパケットヘッダだけでなく、パケットのペイロード（データ部）にも埋め込まれるタイプのアプリケーション向けの機能
  - シングル-エンド-ポイントしか指定できないVPN装置に対しても、回線負荷分散の構成を提供するための機能

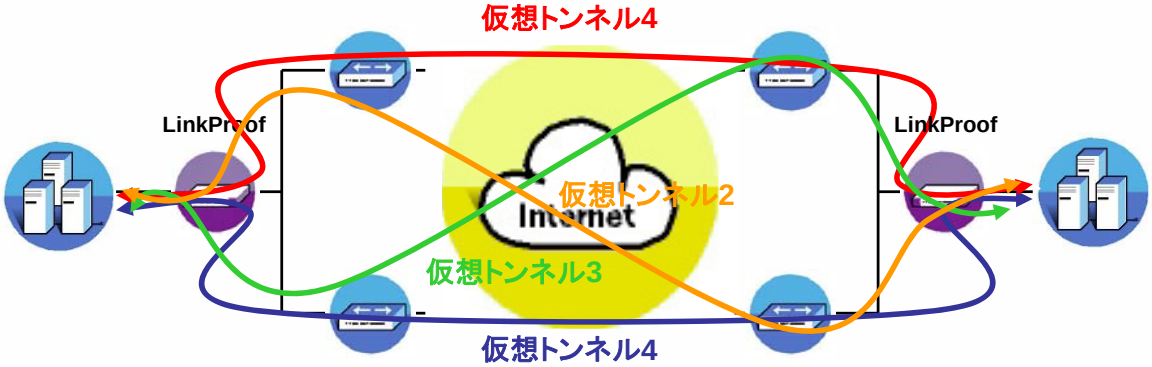
- ペイロードにアドレスが埋め込まれるタイプのアプリケーションは、なぜNATデバイス越えができないのか？
  - NATされたソースアドレスとペイロードに埋め込まれたオリジナルのアドレスが違う場合、宛先サーバにおいて、そのパケットは破棄され、通信が成り立ちません



- シングル-エンド-ポイントしか指定できないVPN装置に、なぜ回線負荷分散の構成が提供できないのか？
  - 一方のサイトでマルチホーミング構成を取っていても、そこにアクセスしてくるVPN装置が、対向のアドレスを1つしか設定できない場合、使用中のISP経由の通信に障害が発生した時、自動的に相手先を切り替えることが出来ない



- 仮想トンネリング動作内容
  - 前記の問題を解決するために、サイト間にLinkProof を配置し、仮想トンネル間で、パケットをカプセル化してトラフィックをやり取りします
  - カプセル化をする際に、ソースアドレスとディスティネーションアドレスの両方をNATします



- 回線障害時の動き
  - トンネルのヘルスチェックが失敗する
  - クライアントテーブルの該当エントリ消え、新たなクライアントテーブルが作成される
  - それに伴い、カプセル化するNATアドレスを変更する
  - カプセル化するNATアドレスは、送信先に届くアドレスには影響を与えないので、End-to-Endで通信が滞ることはない

- TRP（トンネリング レポート プロトコル）
  - LinkProof独自の内部通信用プロトコル
  - 仮想トンネルの構築、維持のために使用される
  - LinkProof間で、UDP 2090を使用して行う

LinkProof 導入シナリオ

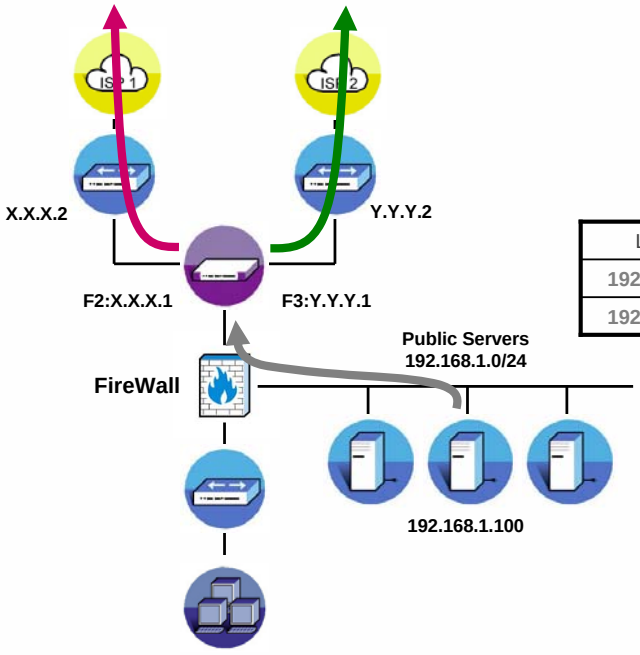
Smart Network. Smart Business.

radware | 導入シナリオ

Smart Network. Smart Business.

- 導入シナリオ
  - シナリオ1
    - 新規構築シナリオ
  - シナリオ2
    - ISP回線 追加シナリオ（既存回線あり）

- シナリオ1
  - インターネット周りを新規構築
  - インターネットへの回線はISP1、ISP2の2回線を用意
  - ISP1から割り当てられたアドレス　X.X.X.0/24
  - ISP2から割り当てられたアドレス　Y.Y.Y.0/24

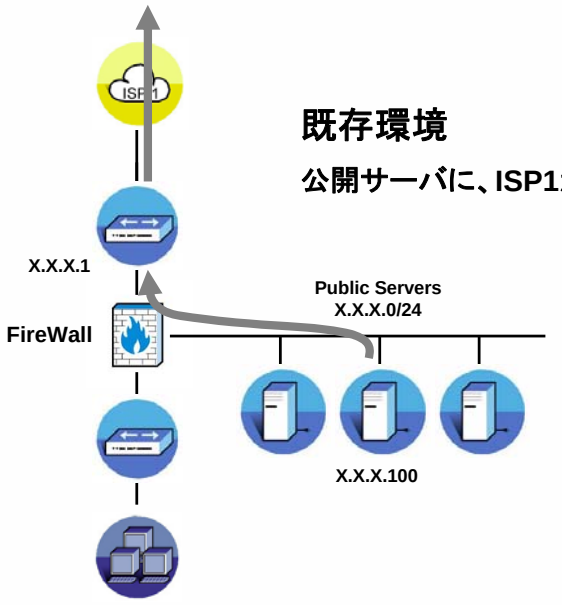


ISP1経由で出て行く場合は、
ISP1のGlobal IPでStatic NAT
して出て行く

Local IP	Static NAT IP	Router IP
192.168.1.100	X.X.X.100	X.X.X.2 (ISP1)
192.168.1.100	Y.Y.Y.100	Y.Y.Y.2 (ISP2)

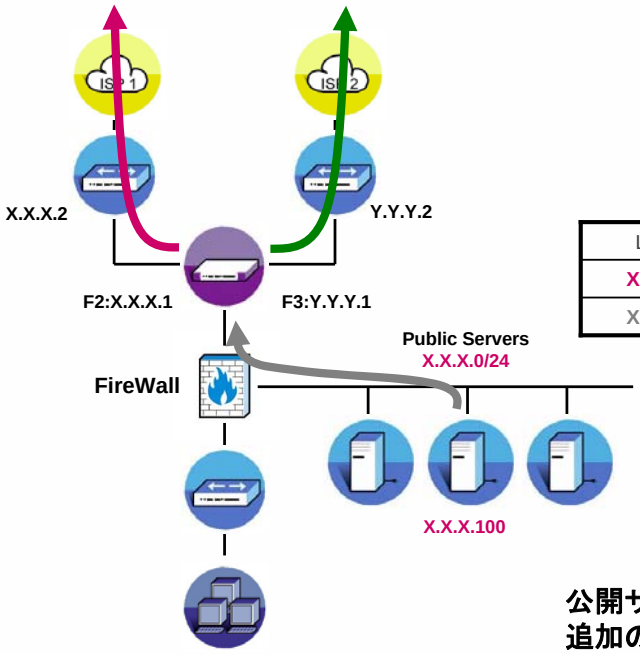
ISP2経由で出て行く場合は、
ISP2のGlobal IPでStatic NAT
して出て行く

- シナリオ2
  - 既に1回線のインターネット接続がある
  - 既存ISP1から割り当てられたアドレス　　X.X.X.0/24
  - 新規にISP2と契約し、2回線目追加
  - 新規ISP2から割り当てられたアドレス　　Y.Y.Y.0/24
  - 公開サーバには、ISP1のGlobal IPを付加済み



既存環境

公開サーバに、ISP1から割り当てられたGlobal IPを付加



ISP1経由で出て行く場合は、
NATせず、そのまま出て行く(No NAT)

Local IP	Static NAT IP	Router IP
X.X.X.100	X.X.X.100	X.X.X.1 (ISP1)
X.X.X.100	Y.Y.Y.100	Y.Y.Y.1 (ISP2)

ISP2経由で出て行く場合は、
ISP2のGlobal IPでStatic NAT
して出て行く

**公開サーバのアドレスを変更することなく
追加の回線を収容する事ができる**

radware
availability | performance | security

Smart Network. Smart Business.