

Equalizer E450 + Webshield e500  
検証結果報告



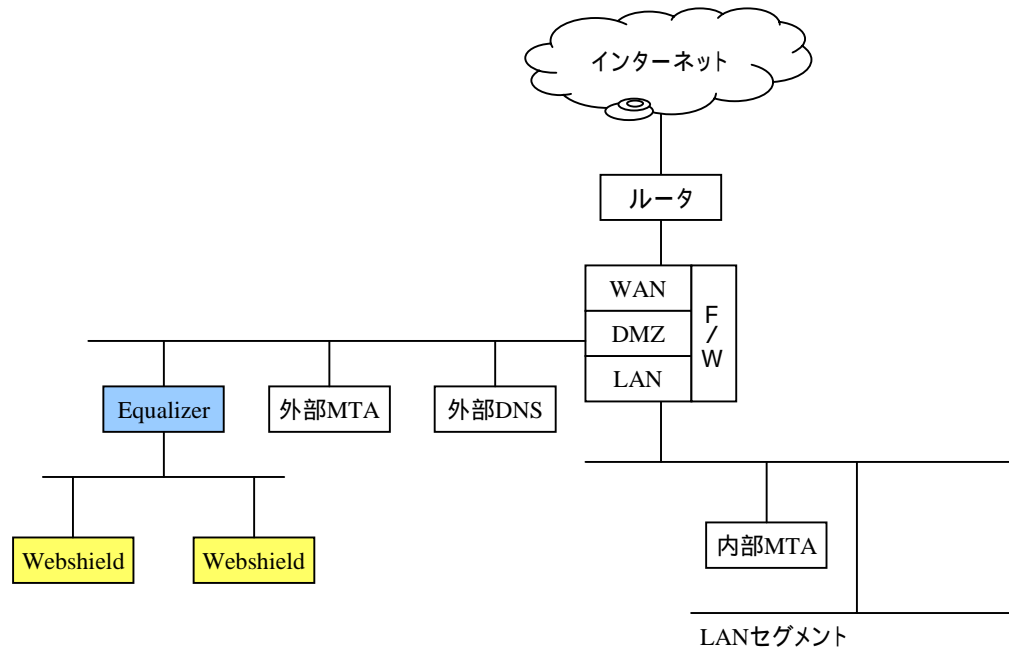
**Networld, Inc.**

# Equalizer + Webshield Appliance 構成パターン

EqualizerでWebshield Applianceの負荷分散を行う場合、  
Webshield ApplianceをProxyモードで設定し構成する。

# Equalizer + Webshield構成パターン メール(1)

- 外部MTA、内部MTAによるWebshieldのサンドイッチ構成

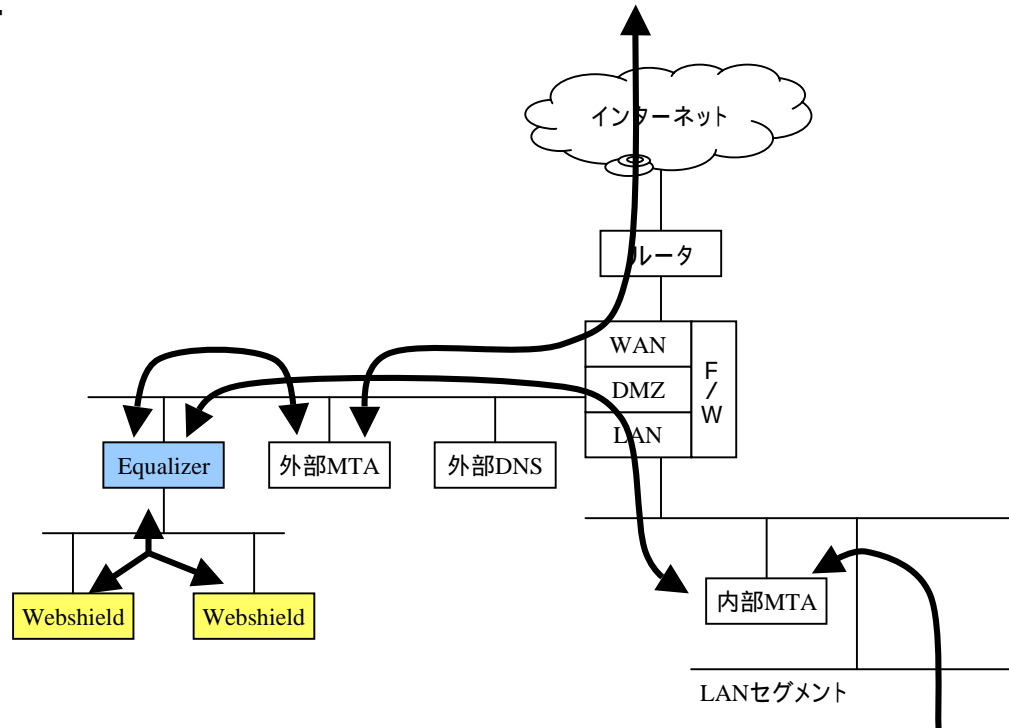


- 外部DNSのMXレコードとして外部MTAを設定し、外部MTAよりWebshieldクラスタIP(\*)へ配信を行う構成。
- 既存構成、設定の変更が必要です。  
Equalizerのアドレスアサイン、MTAの配信設定、DNSのレコード、F/Wのポリシーなど。
- LANセグメント内にサブドメインを複数設定し、Webshieldから配信制御することも可能です。

(\*)クラスタIPとは、Equalizerにおける、バーチャルIPアドレスのことです。

# Equalizer + Webshield構成パターン メール(1)

## ・データフロー



### <メール送信>

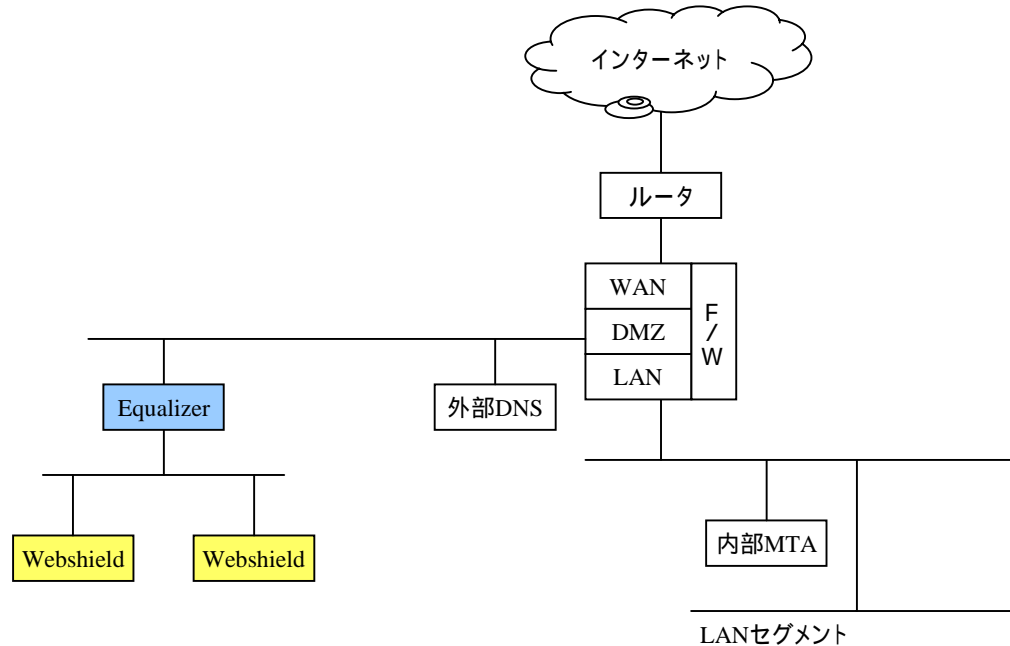
LANセグメントのクライアント 内部MTA : クライアントのメール送信  
内部MTA WebshieldクラスIP : 外部へのメール配信  
Equalizerによる負荷分散  
EqualizerリアルIP (WebshieldリアルIPをSourceNAT) 外部MTA  
: 外部へのメール配信  
外部MTA インターネット : インターネットへのメール配信

### <メール受信>

インターネット 外部MTA : インターネットからのメール配信  
外部MTA WebshieldクラスIP : ローカルドメインへのメール配信  
Equalizerによる負荷分散  
EqualizerリアルIP (WebshieldリアルIPをSourceNAT) 内部MTA  
: ローカルドメインへのメール配信

# Equalizer + Webshield構成パターン メール(2)

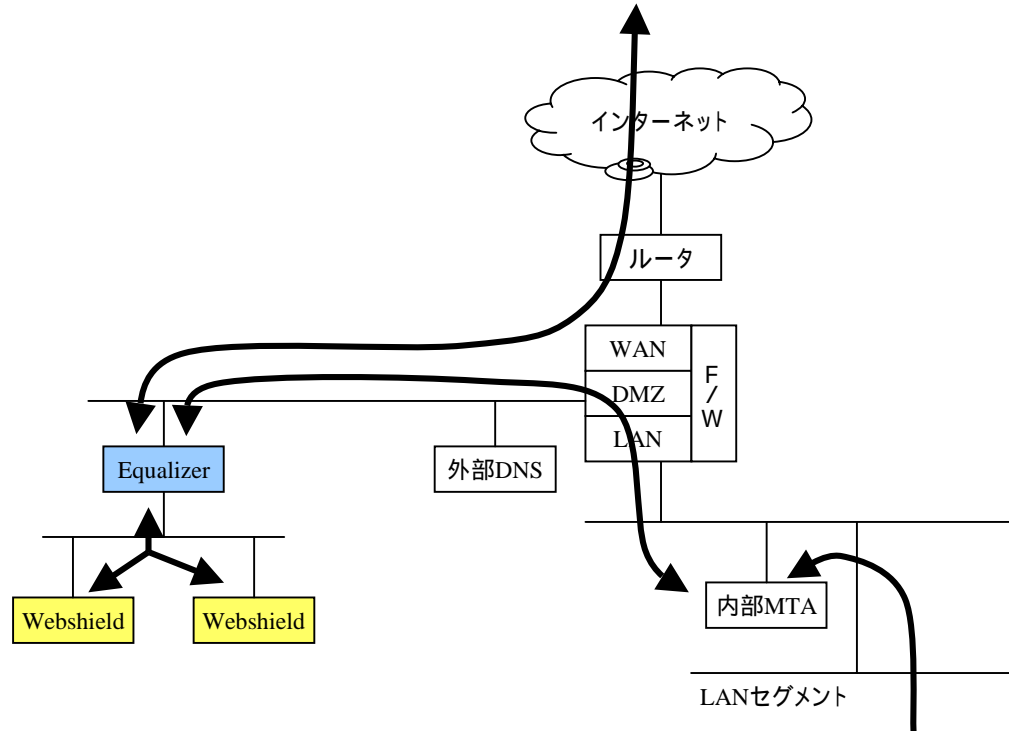
## ・Webshieldによる外部MTAリプレース構成



- ・外部DNSのMXレコードとしてWebshieldクラスタIPを設定し、Webshieldより内部MTAへ配信を行う形です。
- ・既存構成、設定変更が少なくて少なくて済む構成です。( Equalizerのアドレスアサイン程度)
- ・LANセグメント内にサブドメインを設定し、Webshieldから配信制御することも可能。
- ・外部DNSにワイルドカードMXを設定し、Webshieldをメールゲートウェイのような形にして各サブドメインへ配送させる構成も可能。
- ・Webshieldに外部MTAとして直接インターネット上のMTAと配信を行わせる場合には、不正中継対策、SPAM対策などの配送制御を十分に行う必要があります。

# Equalizer + Webshield構成パターン メール(2)

## ・データフロー



### <メール送信>

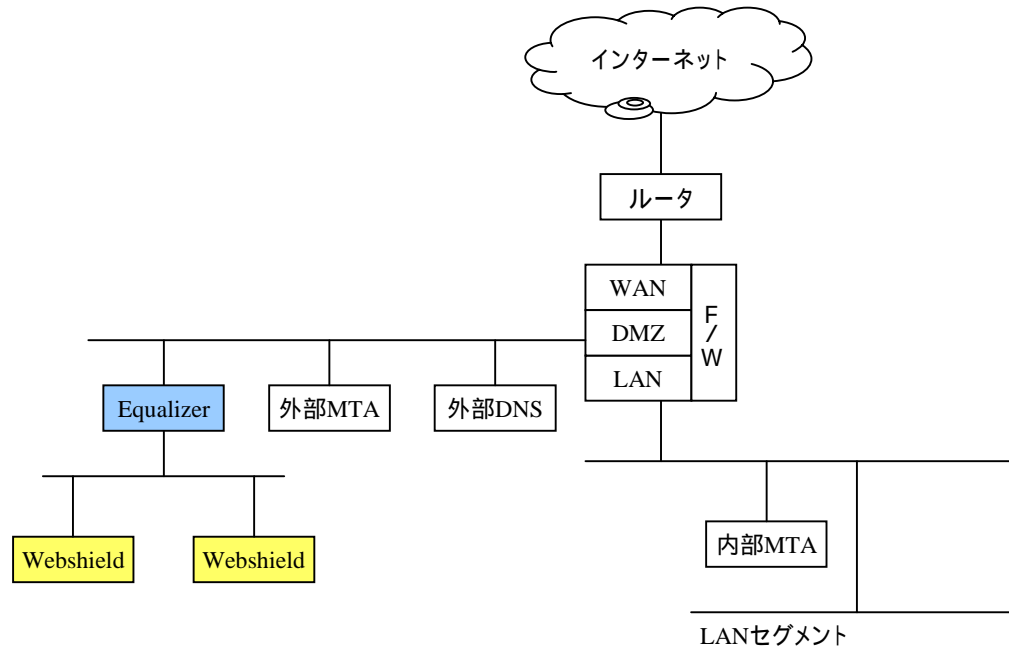
LANセグメントのクライアント 内部MTA : クライアントのメール送信  
内部MTA WebshieldクラスタIP : 外部へのメール配信  
Equalizerによる負荷分散  
EqualizerリアルIP (WebshieldリアルIPをSourceNAT) インターネット  
: 外部へのメール配信

### <メール受信>

インターネット WebshieldクラスタIP  
: インターネットからのメール配信  
Equalizerによる負荷分散  
EqualizerリアルIP (WebshieldリアルIPをSourceNAT) 内部MTA  
: ローカルドメインへのメール配信

# Equalizer + Webshield構成パターン メール(3)

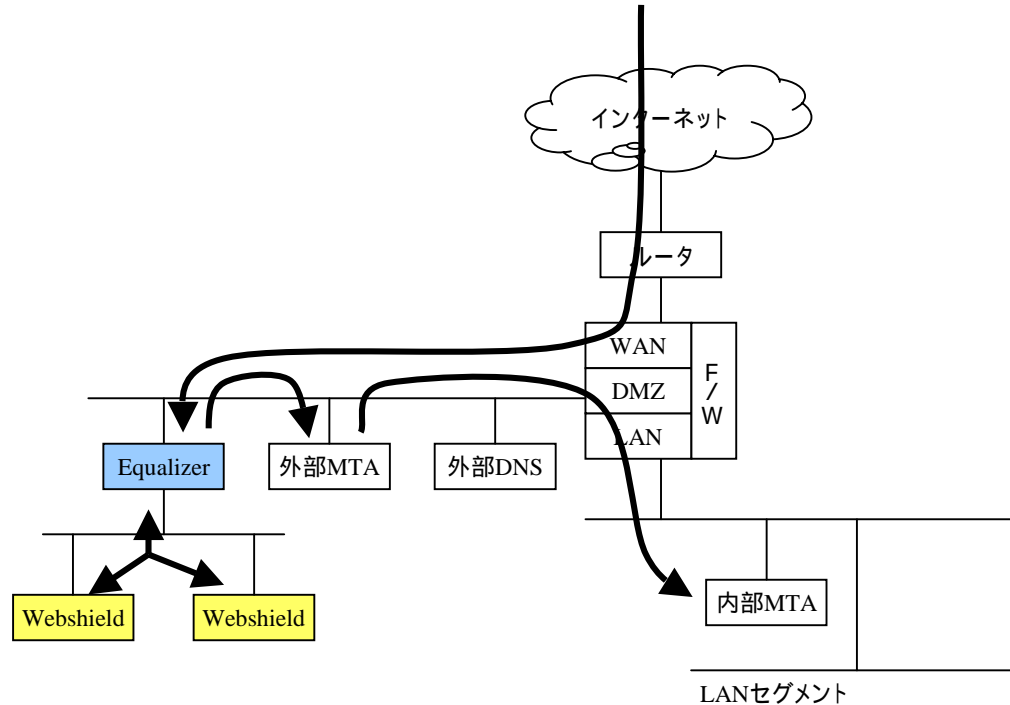
- ・受信と受信時の外部MTAが異なる構成  
(受信のみWebshieldがインターネットから直接)



- ・受信のみWebshieldへ直接インターネットから配信を行う。インターネット送信は既存の外部MTAにより行う
- ・ウイルスメールの受信処理を外部MTAが行わずに済む点、Webshieldから直接内部MTAへの通信がない点などがメリット。  
(内部MTAからWebshieldへの通信あり)
- ・外部DNSのMXレコードとしてEqualizerクラスターIPを設定する。
- ・既存構成、設定の変更が必要です。 Equalizerのアドレスアサイン、MTAの配信設定、DNSのレコード、F/Wのポリシーなど。

# Equalizer + Webshield構成パターン メール(3)

## ・データフロー



### <メール受信>

インターネット WebshieldクラスターIP : インターネットからのメール配信

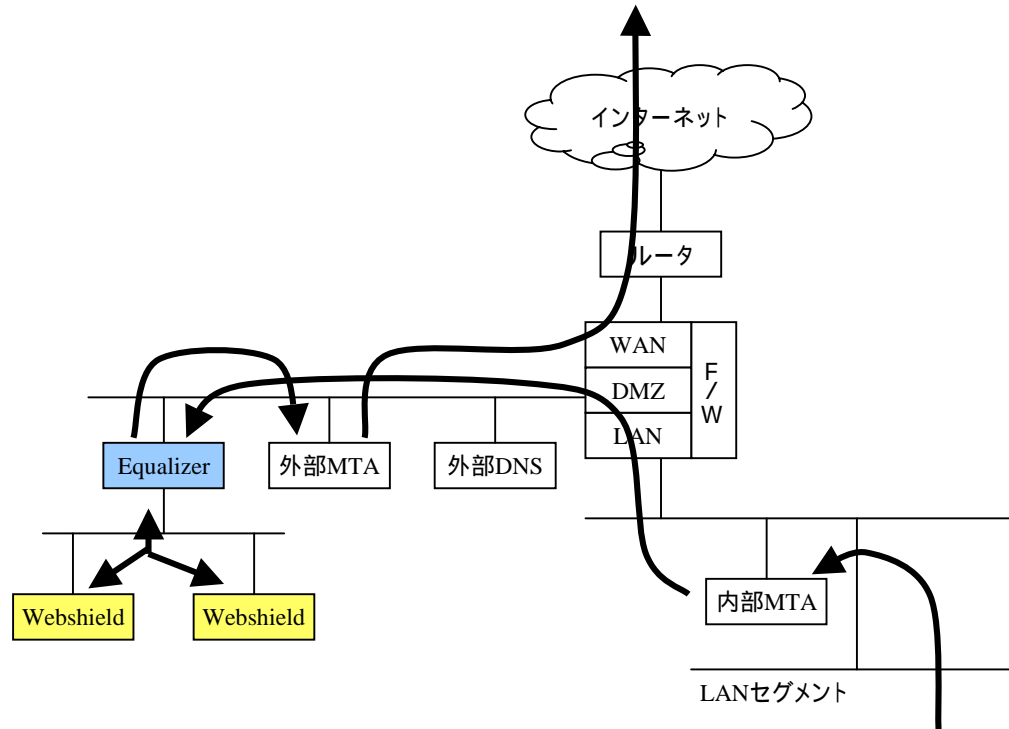
Equalizerによる負荷分散

EqualizerリアルIP (WebshieldリアルIPをSourceNAT) 外部MTA : ローカルドメインへのメール配信

外部MTA 内部MTA : ローカルドメインへのメール配信

# Equalizer + Webshield構成パターン メール(3)

## ・データフロー



### <メール送信>

LANセグメントのクライアント 内部MTA : クライアントのメール送信

内部MTA WebshieldクラスIP : 外部へのメール配信

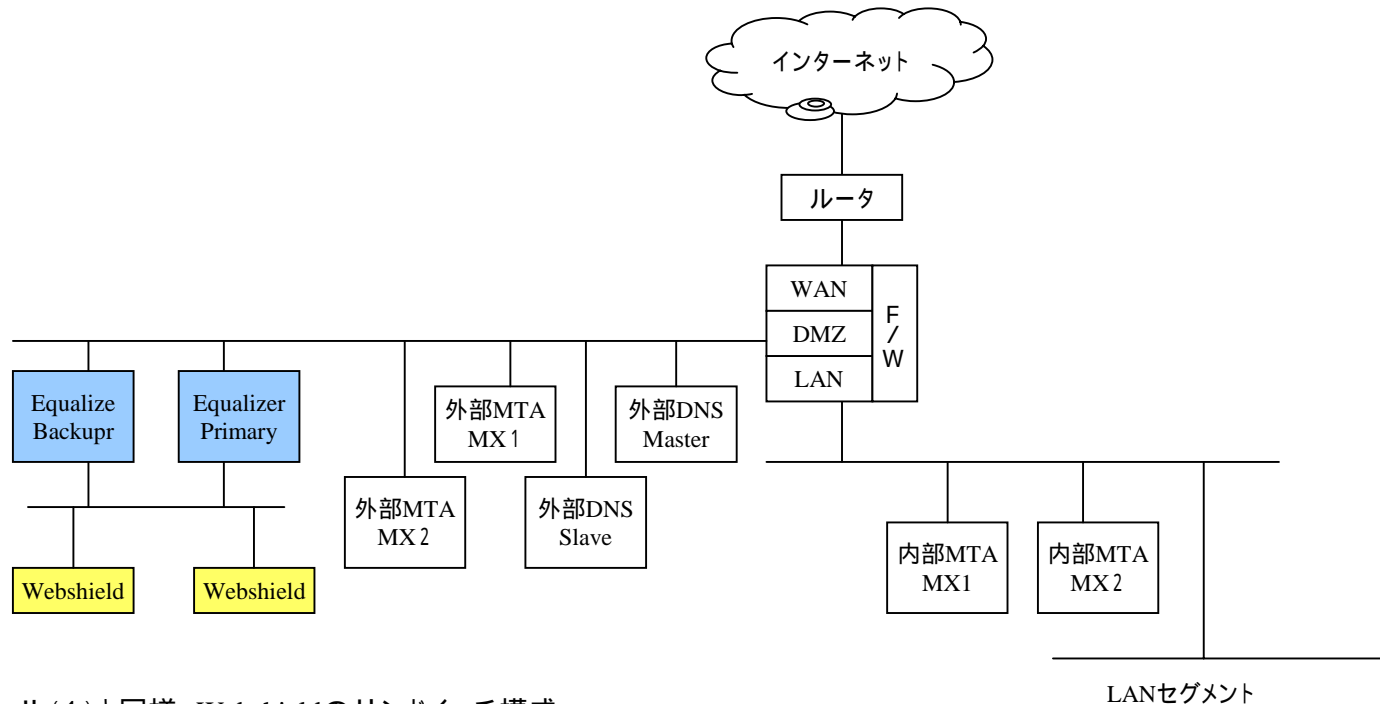
Equalizerによる負荷分散

EqualizerリアルIP (WebshieldリアルIPをSource NAT) 外部MTA : 外部へのメール配信

外部MTA インターネット : インターネットへのメール配信

# Equalizer + Webshield構成パターン メール(4)

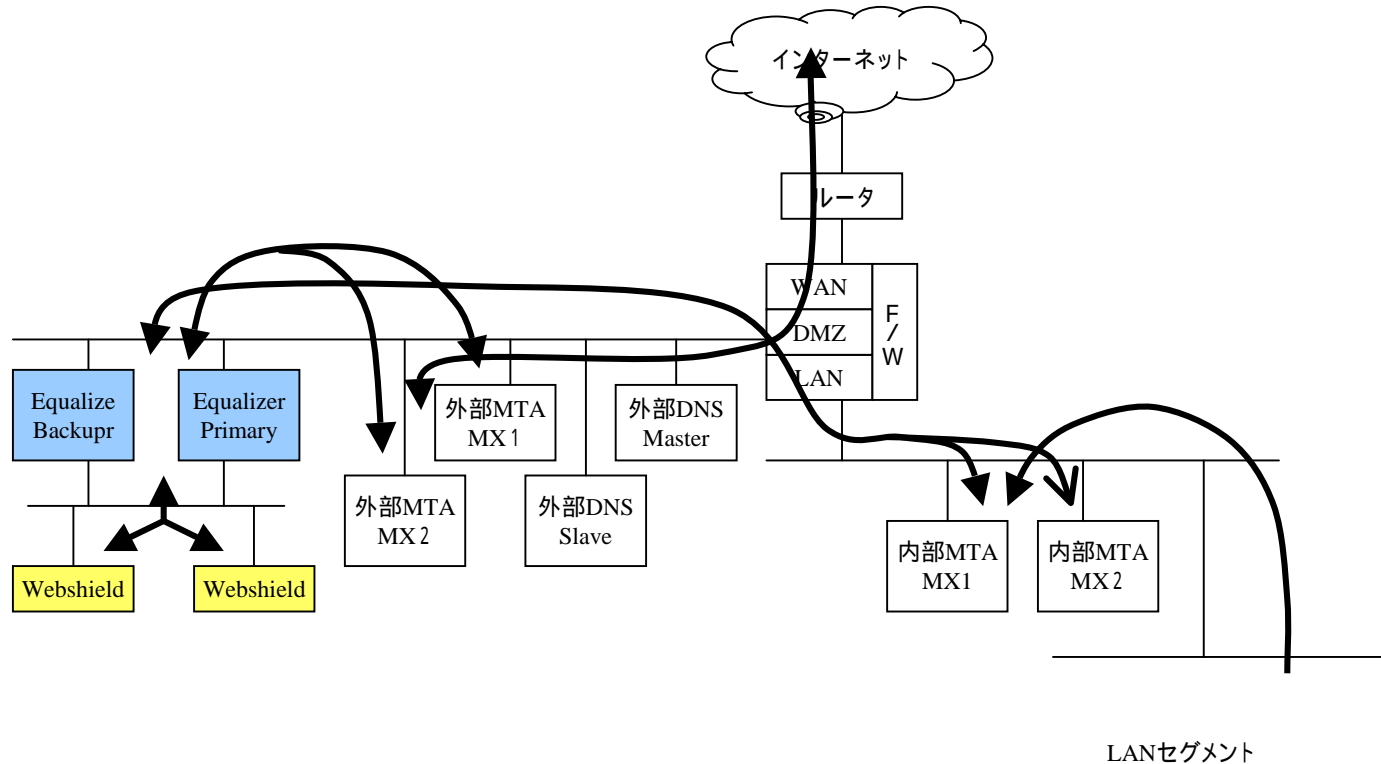
Equalizer、外部、内部MTAを含めたメール配信の二重化構成



- ・構成はメール(1)と同様、Webshieldのサンドイッチ構成
- ・各ネットワーク機器の二重化
  - Equalizerの負荷分散によるWebshield二重化、Equalier HA構成による二重化、Webshieldのローカルドメイン配信の冗長化機能による内部、外部MTAの二重化
- ・Webshieldから配信先MTAの冗長化
  1. Webshieldのドメイン配信先ホストの冗長化機能を使用(Hotfix12/3より実装)
  2. WebshieldでDNSLookupを行い、DNS上のMXレコードを優先度を付け複数設定

# Equalizer + Webshield構成パターン メール(4)

## ・メール配信データフロー



### <メール送信>

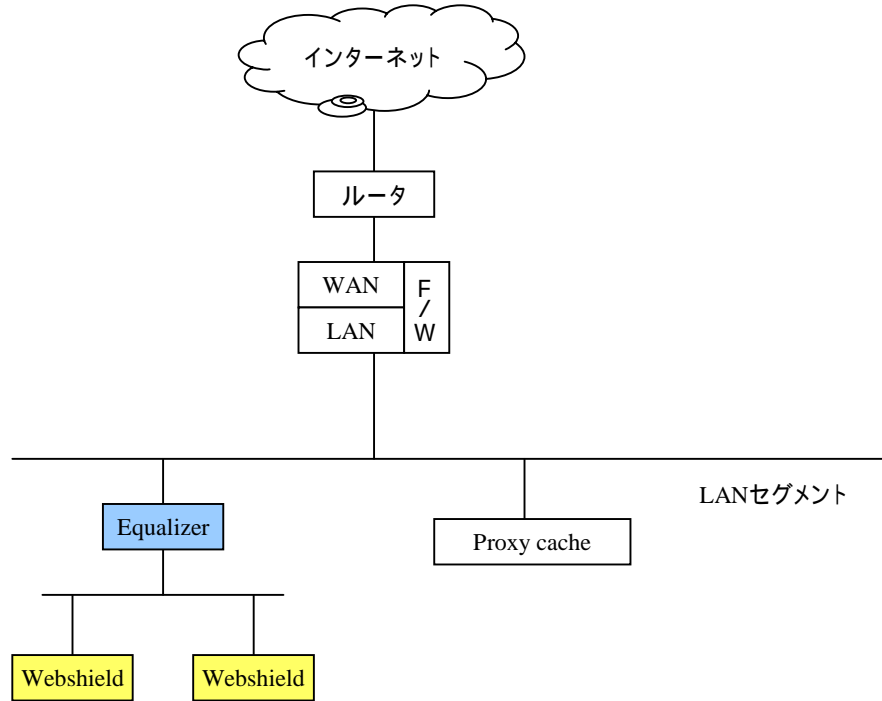
LANセグメントのクライアント 内部MTA : クライアントのメール送信  
 内部MTA WebshieldクラスターIP : 外部へのメール配信  
 Equalizerによる負荷分散  
 EqualizerリアルIP (WebshieldリアルIPをSourceNAT) 外部MTA  
 : 外部へのメール配信 (外部MTA MX1配信失敗時はMX2へ配信)

### <メール受信>

インターネット 外部MTA : インターネットからのメール配信  
 (外部MTAはDNSのMXレコードにより冗長化)  
 外部MTA WebshieldクラスターIP : ローカルドメインへのメール配信  
 Equalizerによる負荷分散  
 EqualizerリアルIP (WebshieldリアルIPをSourceNAT) 内部MTA  
 : ローカルドメインへのメール配信 (内部MTA MX1配信失敗時はMX2へ配信)

# Equalizer + Webshield構成パターン HTTP Proxy (1)

## ・多段Proxy構成



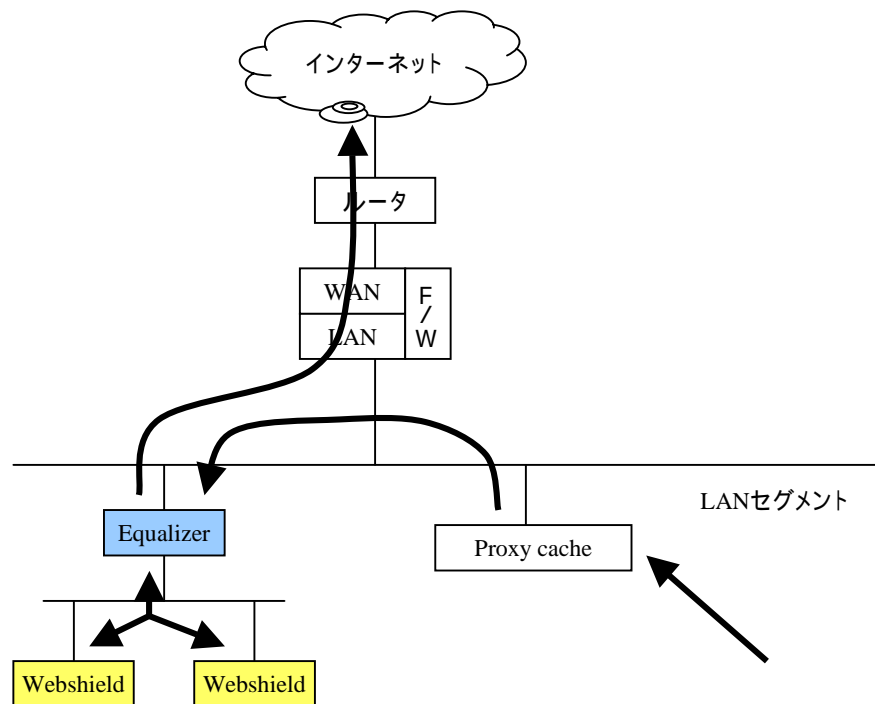
- ・既存非透過型Proxyの親ProxyとしてWebshieldを導入する、もしくはWebshieldの手前にProxy Cacheサーバを導入する構成。
- ・Proxy Cache(もしくは既存Proxy)は親ProxyとしてWebshieldクラスターIPを設定します。既存Proxyの場合はキャッシュを有効に使うこと可能。
- ・既存構成の変更個所として下記が想定されます。

クライアントPCのProxy設定に変更なし、Equalizerのアドレスアサイン、既存Proxyの設定変更、F/Wのポリシー変更など。

- ・WebshieldをSMTPと併用する場合はWebshieldとEqualizerをDMZに配置する構成も考えられます。

# Equalizer + Webshield構成パターン HTTP Proxy (1)

## ・データフロー



クライアントPC (Proxy)

Proxy (Webshield クラスターIP)

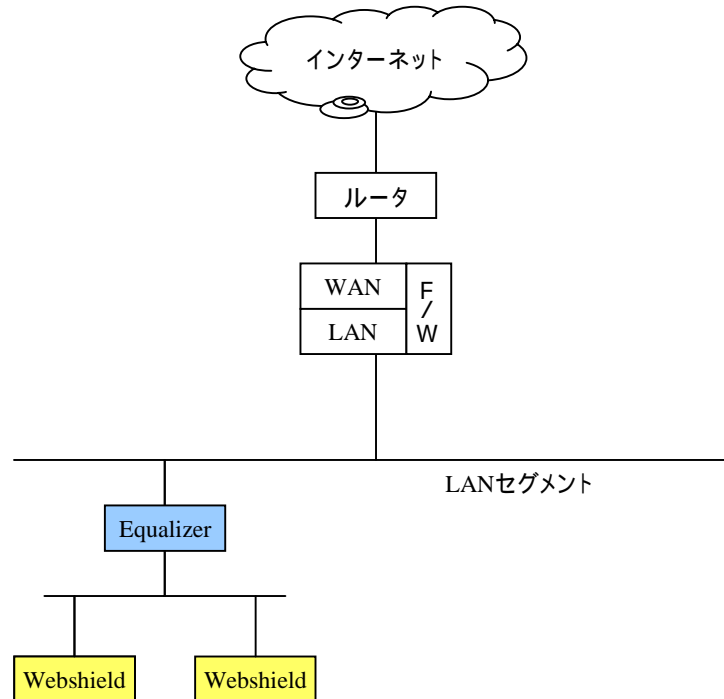
Equalizerによる負荷分散

Equalizer リアルIP (Webshield リアルIP を Source NAT)

インターネット

# Equalizer + Webshield構成パターン HTTP Proxy (2)

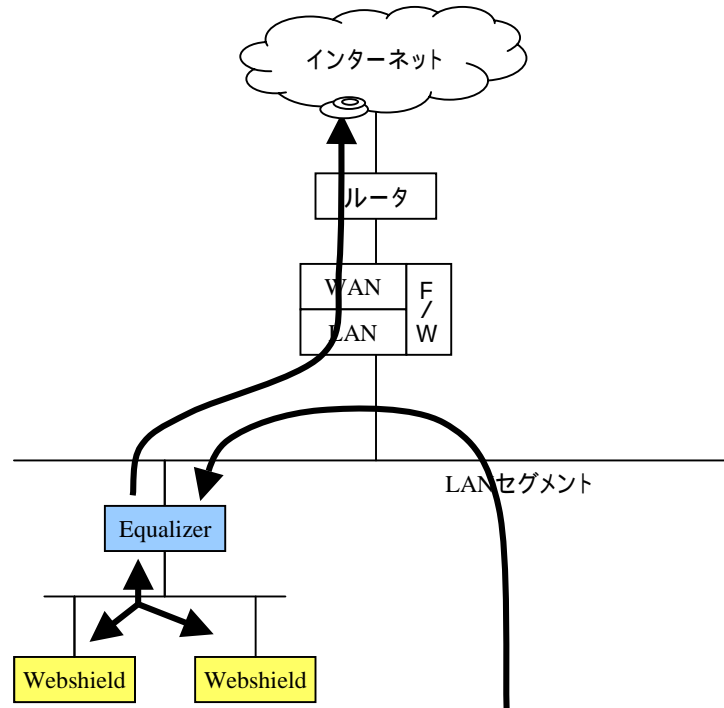
- ・Webshieldによる既存Proxyリブレース構成



- ・既存HTTP Proxyのリブレースとして導入する構成。
- ・WebshieldをSMTPと併用する場合はWebshieldとEqualizerをDMZに配置する構成も考えられます。
- ・既存ProxyのIPをEqualizerクラスターIPに設定することによりクライアントPCのProxy設定の変更が不要。
- ・Proxyキャッシュを有効に使用したい場合は、手前にProxy Cacheサーバを導入する。

# Equalizer + Webshield構成パターン HTTP Proxy (2)

## ・データフロー



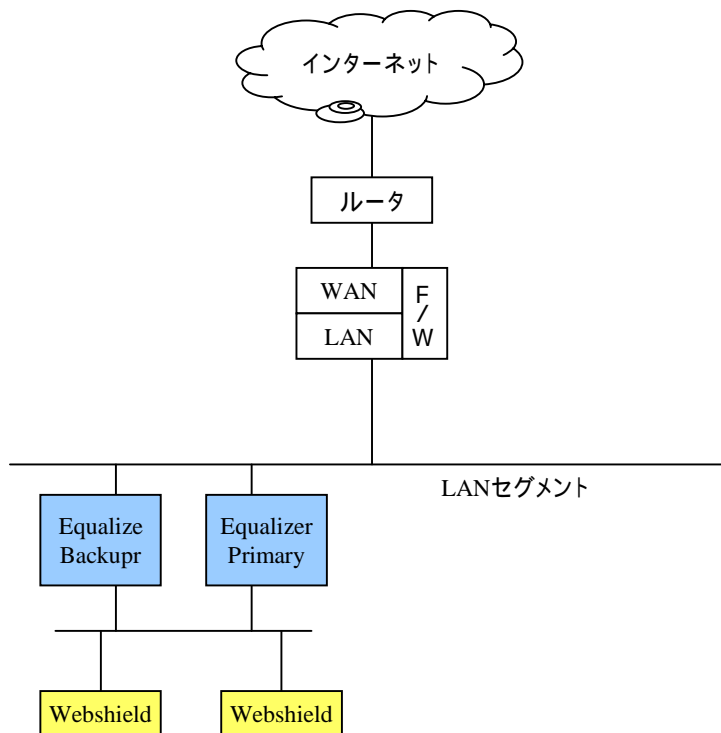
クライアントPC      WebshieldクラスターIP

Equalizerによる負荷分散

EqualizerリアルIP (WebshieldリアルIPをSourceNAT)      インターネット

# Equalizer + Webshield構成パターン HTTP Proxy (2)

・Equalizer二重化構成

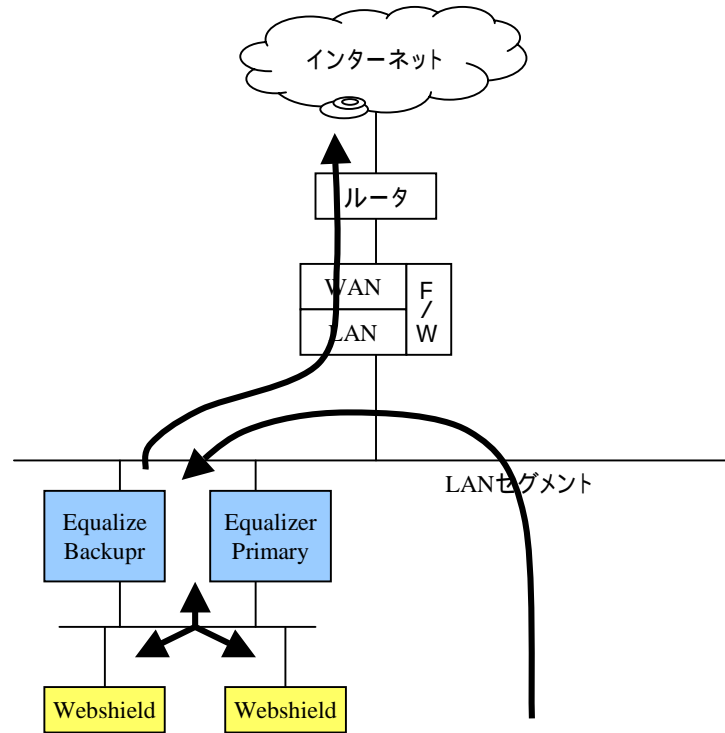


・Equalizer HAによる二重化構成

・多段Proxy構成でも可能(子ProxyはWebshieldクラスタIPを親Proxyとして設定)

# Equalizer + Webshield構成パターン HTTP Proxy (2)

## ・データフロー



クライアントPC      WebshieldクラスターIP

Equalizerによる負荷分散

EqualizerリアルIP (WebshieldリアルIPをSourceNAT)

インターネット

# Equalizer E450 + Webshield e500 検証

- ・Equalizer E450/E350/E250i のソフトウェア機能は共通
- ・Webshield e250/e500/e1000 のソフトウェア機能は共通

上記により、本検証結果はEqualizer製品群、Webshield Appliance製品群を対象とする。

# テスト概要

## < 目的 >

E450による、e500Proxyモードでの負荷分散を検証。

### (1) メール配信の検証

- ・e450による、e500へのメール配信の負荷分散
- ・分散対象のe500から、外部のMTAへのメールの配信

### (2) HTTPアクセスの検証

- ・e450による、e500へのHTTP Proxyの負荷分散
- ・分散対象の500から、外部のWEBサーバへのアクセス

## < 内容 >

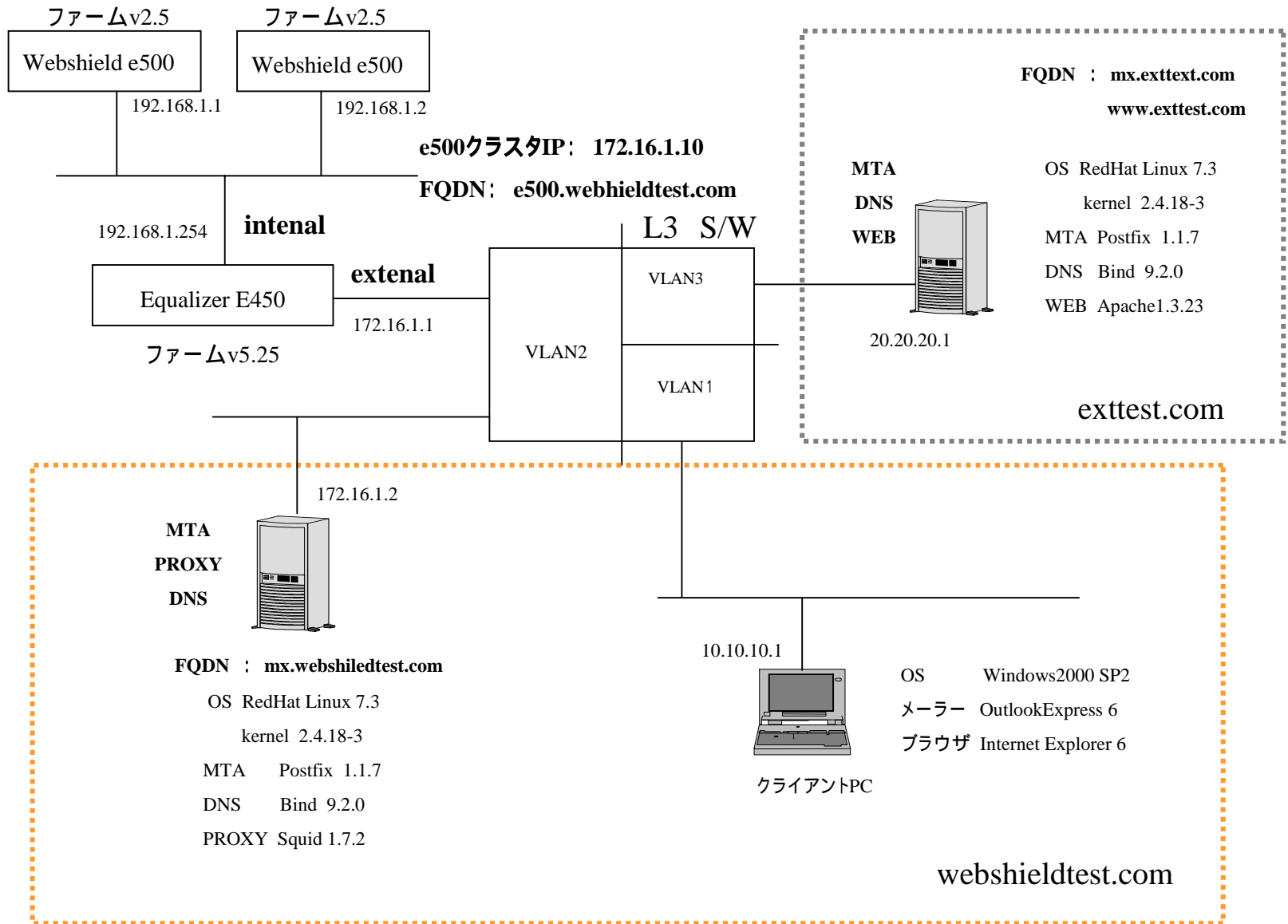
### (1) メール配信の検証

- ・メールの送信、受信両方の中継サーバとしてe500のクラスタIPを設定し、メール配信の負荷分散を行う。

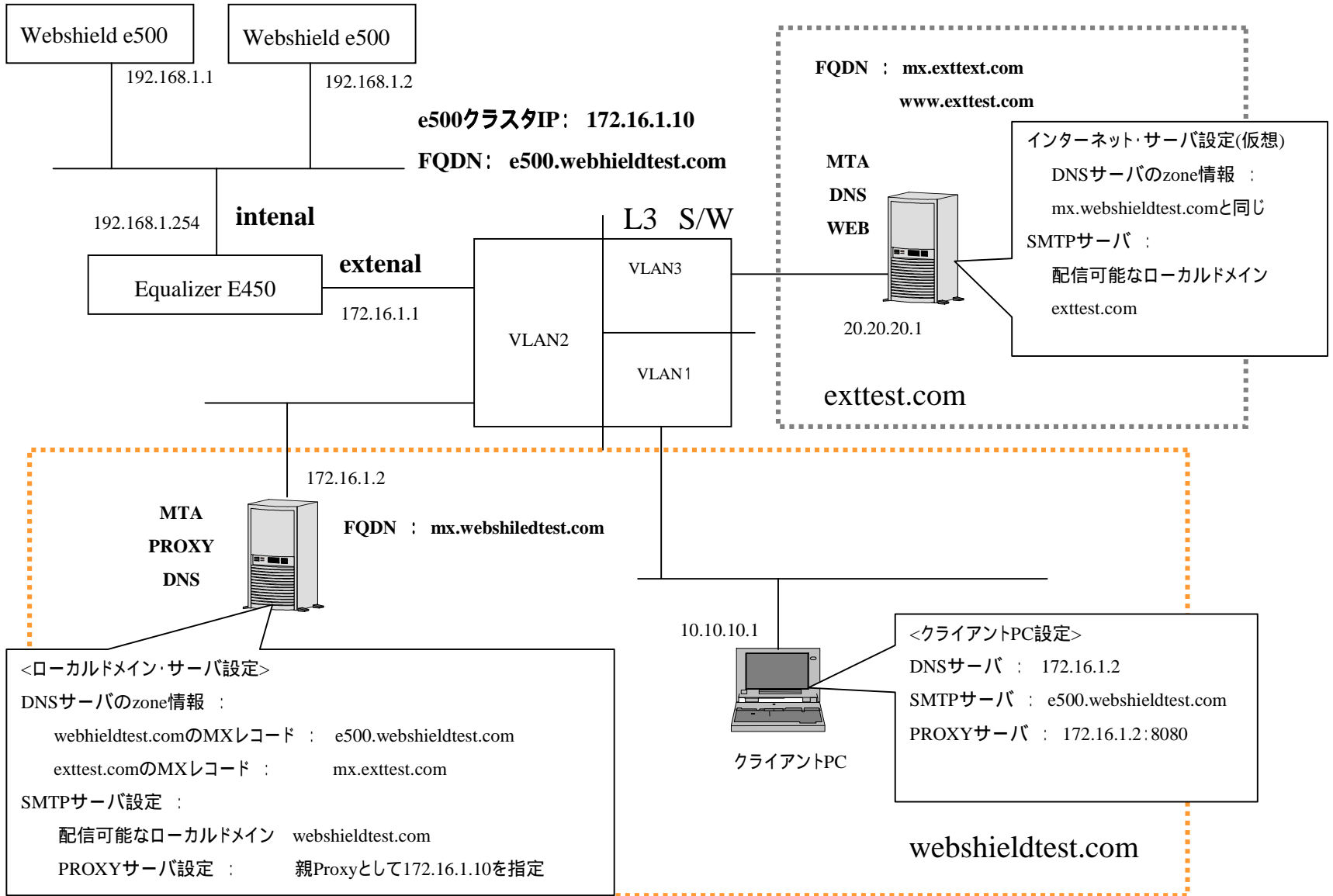
### (2) HTTPアクセスの検証

- ・クライアント設定のProxyサーバの親Proxyとしてe500クラスタIPを設定し、HTTPアクセスの負荷分散を行う。

# テストネットワーク構成



# 各サーバ設定



# E450設定

## 基本設定

- ・OutBoundNAT (SouceIPのNAT) 機能の有効化

外部からルーティングできない internalセグメント上のe500から外部へのメール送信を行うため

## SMTPの負荷分散設定

- ・e500のSMTPのサービスポート、TCP/25でクラスタを作成

TCPポートレベルでの負荷分散

- ・クラスタ・メンバーは2台のe500      192.168.1.1:25   と   192.168.1.2:25

- ・負荷分散負荷分散アルゴリズム      RondRobin

- ・Sticky Time   なし (\*)

(\*)パーシステンス機能。Equalizerのパーシステンスはクライアント・ソースIPによる機能のみ

## HTTPの負荷分散設定

- ・e500のHTTPのサービスポート、TCP/8080のクラスタを作成

TCPポートレベルでの負荷分散

- ・クラスタ・メンバーは2台のe500      192.168.1.1:8080   と   192.168.1.2:8080

- ・負荷分散負荷分散アルゴリズム      RondRobin

- ・Sticky Time   なし

# e500設定

## e500は2台とも全く同じ設定

### 基本設定

- ・DNSとして172.16.1.2を設定 (HTTPアクセスの際に使用)

### SMTPの設定

- ・SMTPをProxyモードで設定
- ・メール配信ルールの設定

メール配信はローカルドメインのみチェック

DNS、代替中継は行わない

ローカルドメインの配信先ホスト

webshieltest.com      mx.webshiedtest.com

\*                      mx.webshieldtest.com

### HTTPの設定

- ・サービスポートを8080で設定
- ・HTTPをProxyモードで設定
- ・ハンドオフホスト(親Proxy)設定      なし(直接外部へアクセス)

## メール配信の流れ(1)

### <インターネットへのメール送信>

クライアントPCのメーラからtest@exttest.comへメールを送信

メーラは設定されたSMTPサーバe500.webshieldtest.comへメールを送信

- ・e500.webshieldtest.comは、e500のクラスタIPへ名前解決されパケットはE450へ転送
- ・E450はアルゴリズム(RoundRobin)に従い、2台のe500のどちらかに負荷分散

メールを受信したe500は、該当ドメイン(外部宛てなので\*に該当)の配信先ホストへメールを転送

- ・mx.webshieldtest.comへ配信

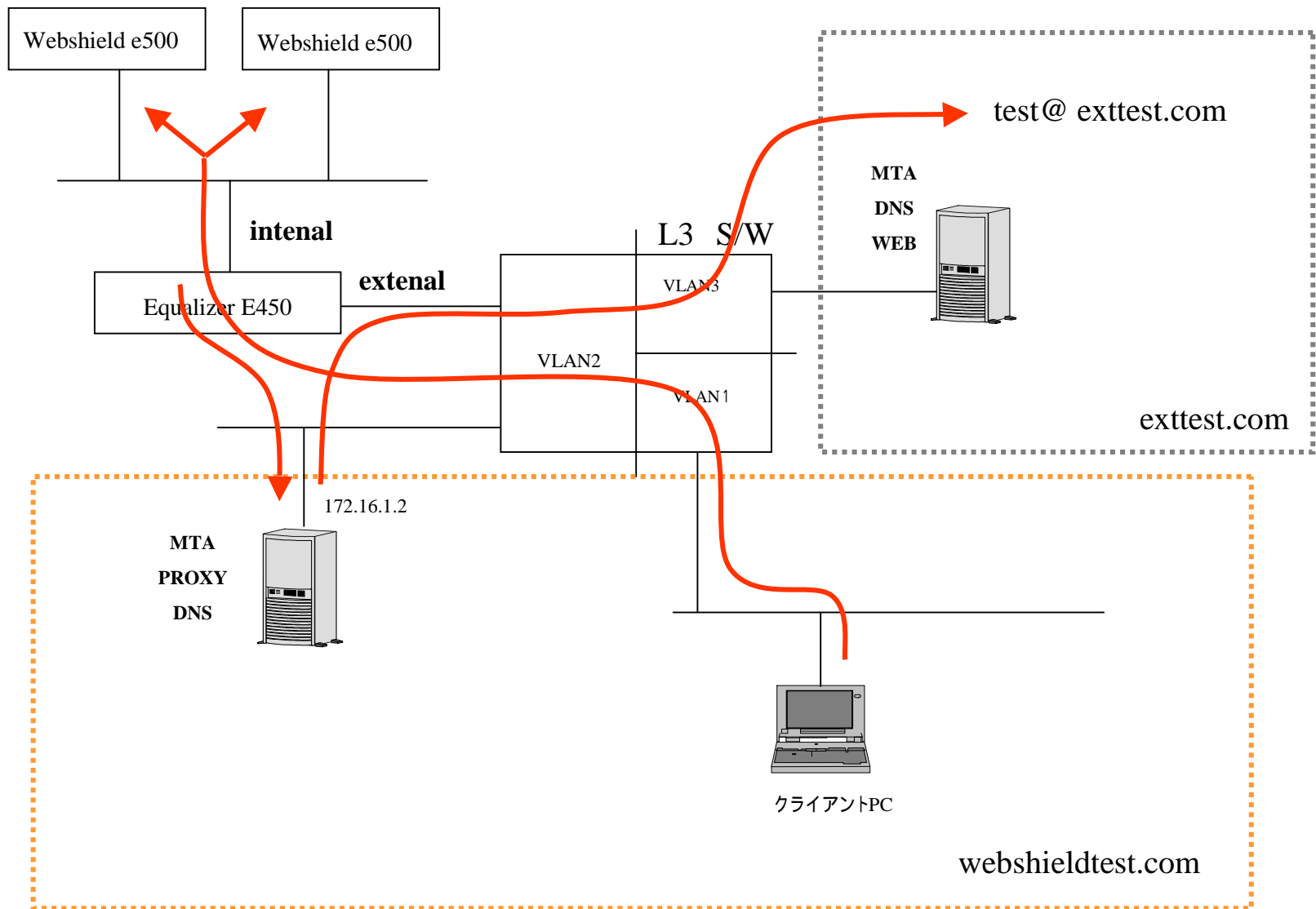
その際、E450から外部へのパケットのソースIPアドレスはE450のOutBoundNAT機能(SourceNAT)により、E450のリアルIPへ変換される。そのため、中継先のMTA上でメール中継するホストの制限をかけている場合は、クラスタIPもしくはホスト名を許可しておくこと。

メールを受信したmx.webshieldtest.comはローカルドメインに該当しないため、DNS-Lookupを行い、

- ・exttest.comのMXレコードに該当するmx.exttest.comへメールを配信
- ・mx.exttest.comはメールを受信し、ユーザtestのメールBOXへメールを格納する。

mx.exttest.comへtestユーザでログインし、mailコマンドでメールを閲覧

# データフロー



## メール配信の流れ(2)

### <インターネットからのメール受信>

mx.extttest.comからmailコマンドで、test@webshIELDtest.comへメールを送信

mx.extttest.comはDNS-LookupによりwebshIELDtest.comのMXレコードに該当する、  
e500.webshIELDtest.comへメールを配信

- ・e500.webshIELDtest.comは、e500のクラスタIPへ名前解決されパケットはE450へ転送
- ・E450はアルゴリズム(RoundRobin)に従い、2台のe500のどちらかに負荷分散

メールを受信したe500は、該当ドメイン(ローカルドメイン宛てなのでwebshIELDtest.comに該当)  
の配信先ホストへメールを転送

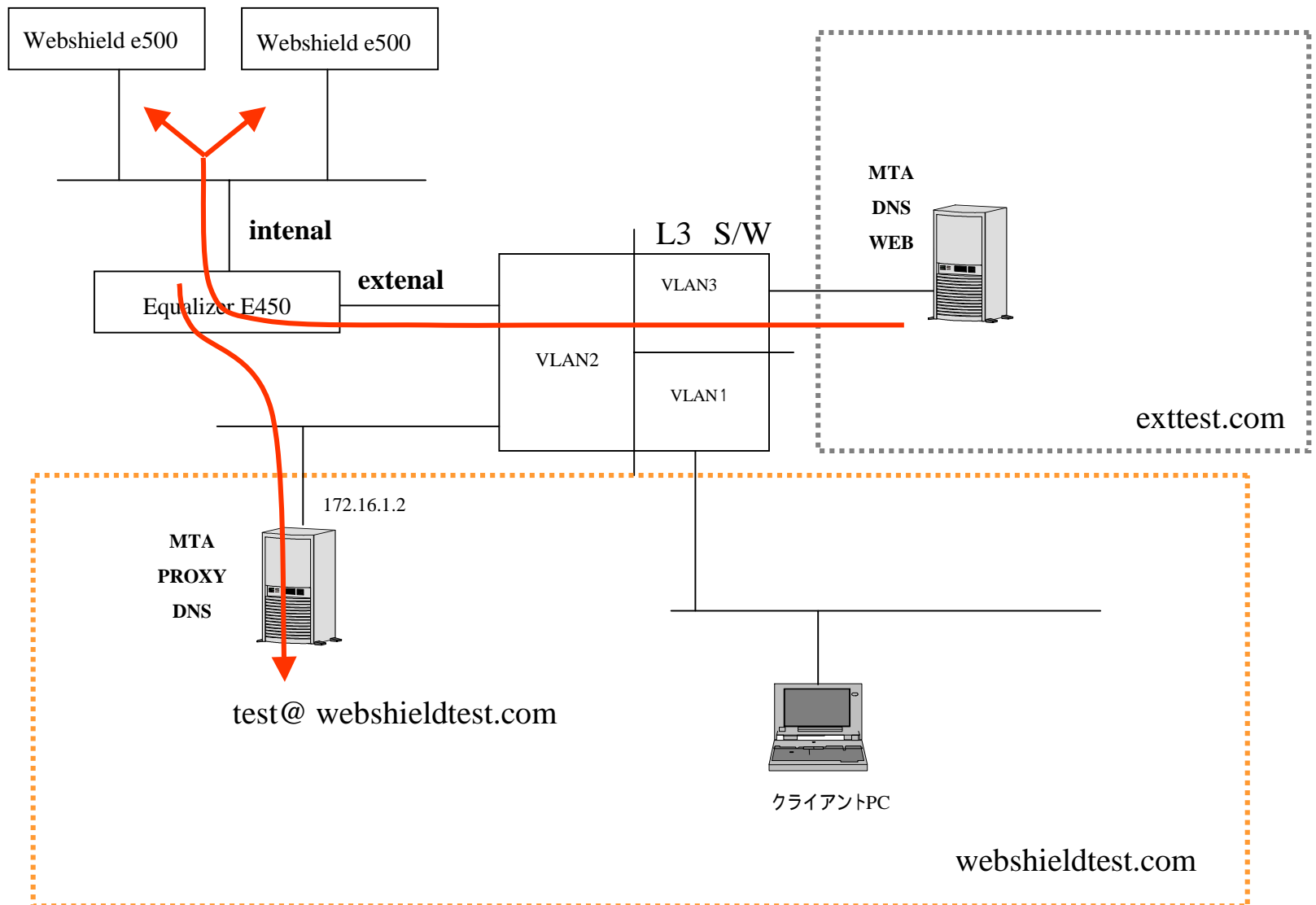
- ・mx.webshIELDtest.comへ配信

その際、E450から外部へのパケットのソースIPアドレスはE450のOutBoundNAT機能  
(SourceNAT)により、E450のリアルIPへ変換される。そのため、中継先のMTA上で  
メール中継するホストの制限をかけている場合は、クラスタIPもしくはホスト名を許可しておくこと。

mx.webshIELDtest.comはメールを受信し、ローカルドメインに該当するため、  
ユーザtestのメールBOXへメールを格納する。

mx.webshIELDtest.comへtestでログインし、mailコマンドでメールBOXの該当メールを閲覧

# データフロー



# HTTPアクセスの流れ

## <インターネットへのHTTPアクセス>

クライアントPCのブラウザより<http://www.exttest.com>へアクセス

クライアントPCより、設定されたProxyサーバ172.16.1.2:8080へアクセス

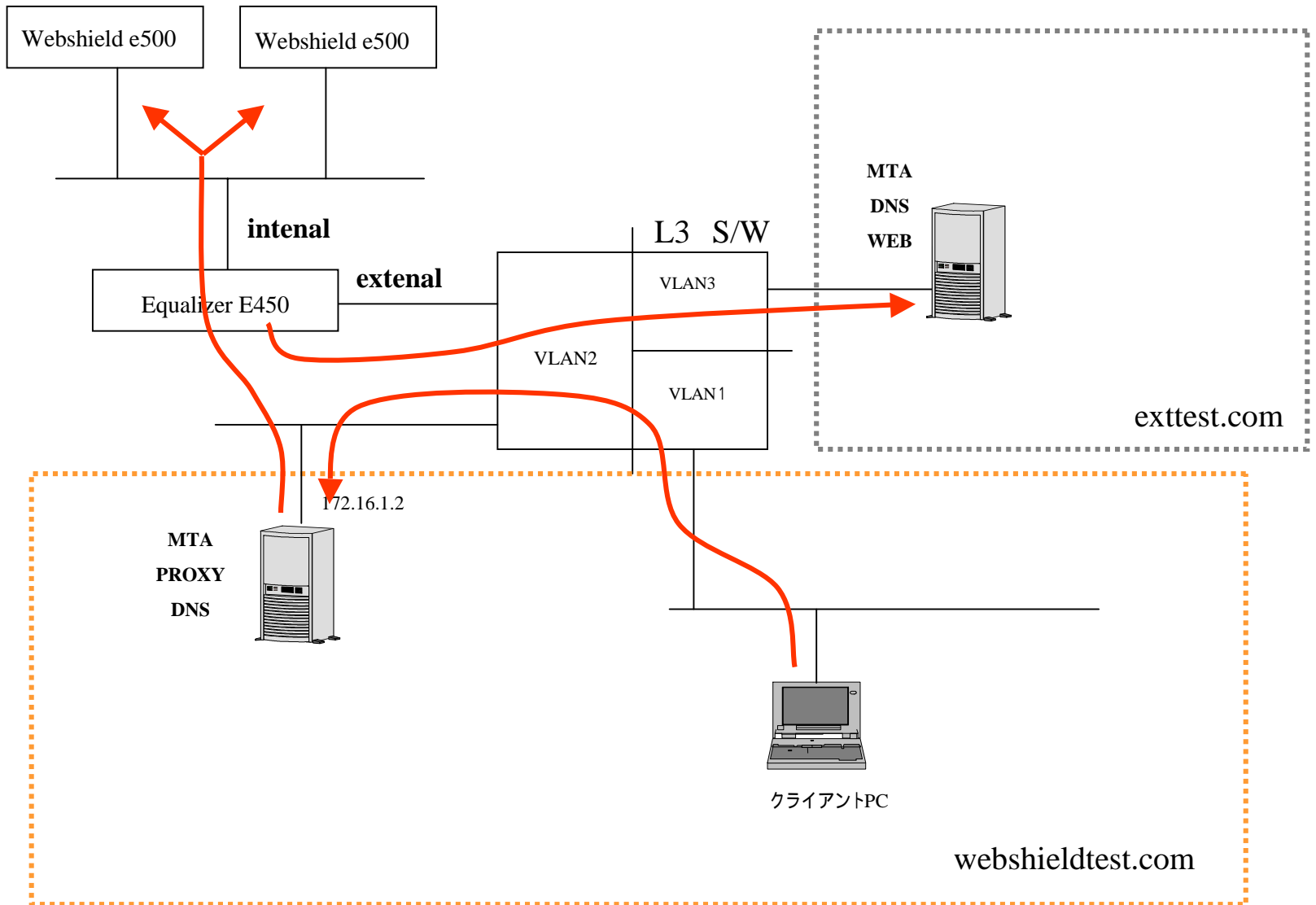
Proxyサーバ172.16.1.2は親Proxyサーバ172.16.1.1:8080へProxyキャッシュをリレー

・172.16.1.2はe500のクラスタIPのため、E450はアルゴリズム(RoundRobin)に従い

2台のe500のどちらかに負荷分散

アクセスされたe500はインターネット上の<http://www.exttest.com>へアクセス

# データフロー



# 検証結果まとめ

## メール配信の負荷分散

- ・EqualizerのTCP / 25番ポートの負荷分散によるe500へのメールの配信OK
- ・e500から外部へのメール配信(EqualizerのOutBoundNAT機能)OK

Equalizerによるメールのロードバランスは成功

MTA配信設定によりネットワーク構成は異なってくるが、上記機能が確認できているため、構成が異なっても問題ないと思われる。

## HTTP Proxyの負荷分散

- ・EqualizerのTCP / 8080番ポートの負荷分散によるe500へのHTTP ProxyアクセスOK
- ・e500から外部へのHTTPアクセスOK

EqualizerによるHTTP Proxyのロードバランスは成功

Proxyキャッシュのリレー設定によりネットワーク構成は異なってくるが、上記機能が確認できているため、構成が異なっても問題ないと思われる。