Managed UTM/FW NG設定例

3.0版

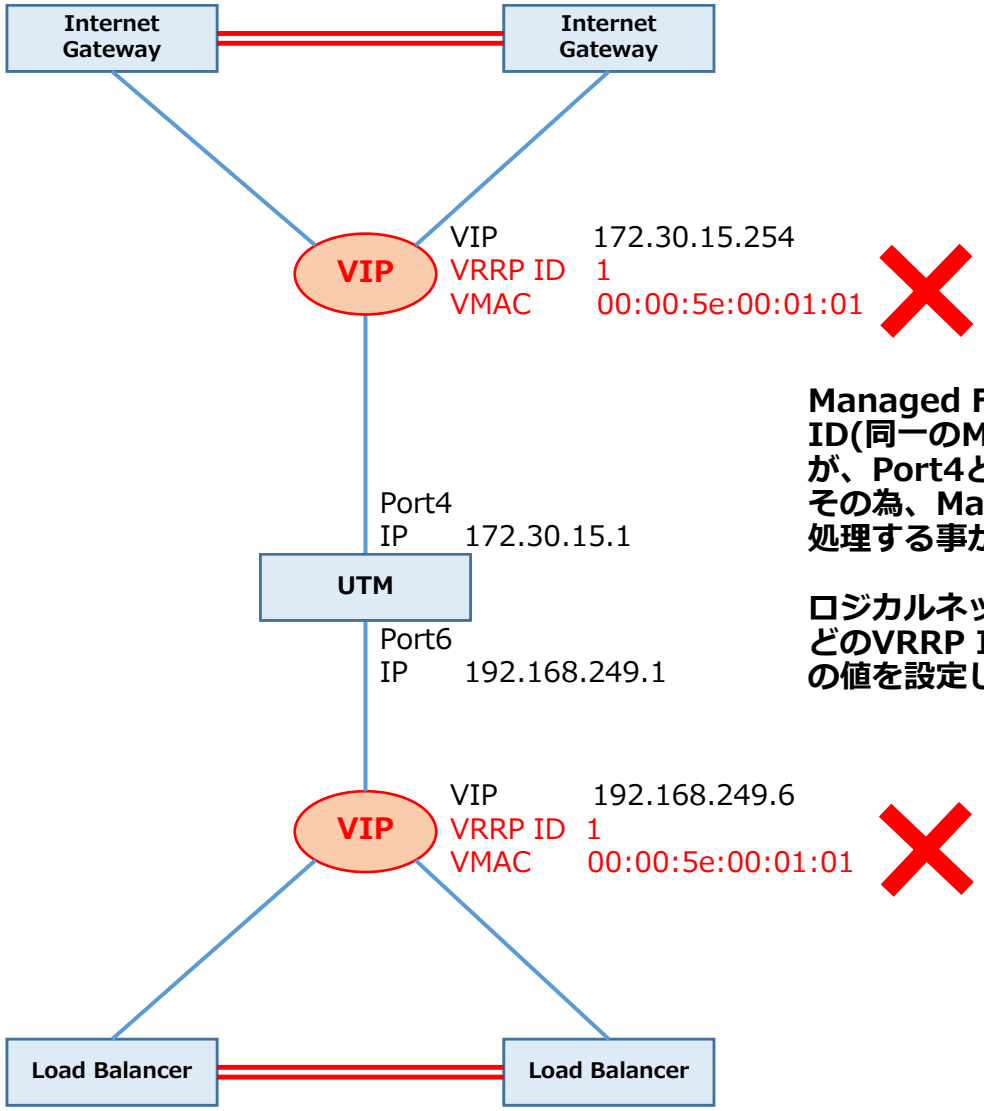
2017/11/15

NTT Communications

更新履歴

版数	更新日	更新内容
1.0	2017/08/08	• 初版
2.0	2017/10/24	• 第2版 NG構成(AWS、VPN-GW接続)の追加
3.0	2017/11/15	• 第3版 NG構成(各種GW接続)の追加

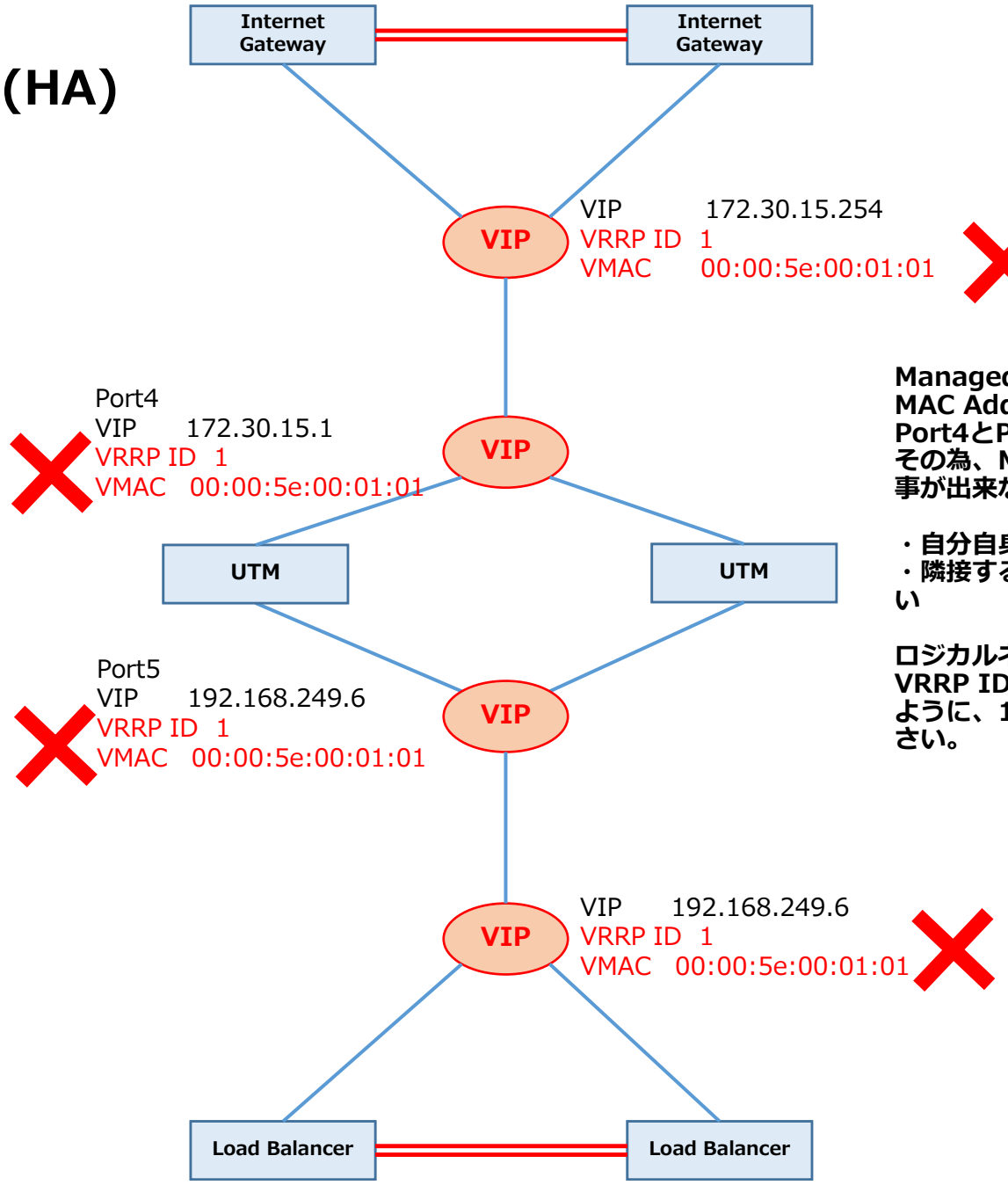
MAC Address重複(Single)



Managed Firewall/UTMからみて、同一のVRRP ID(同一のMAC Address【00:00:5e:00:01:01】)が、Port4とPort5の先に存在する。
その為、Managed Firewall/UTMは正常にPacketを処理する事が出来ない。

ロジカルネットワーク上の他メニュー/持ち込み製品などのVRRP IDは、11以外の値で、1、2のように別々の値を設定してください。

MAC Address重複(HA)

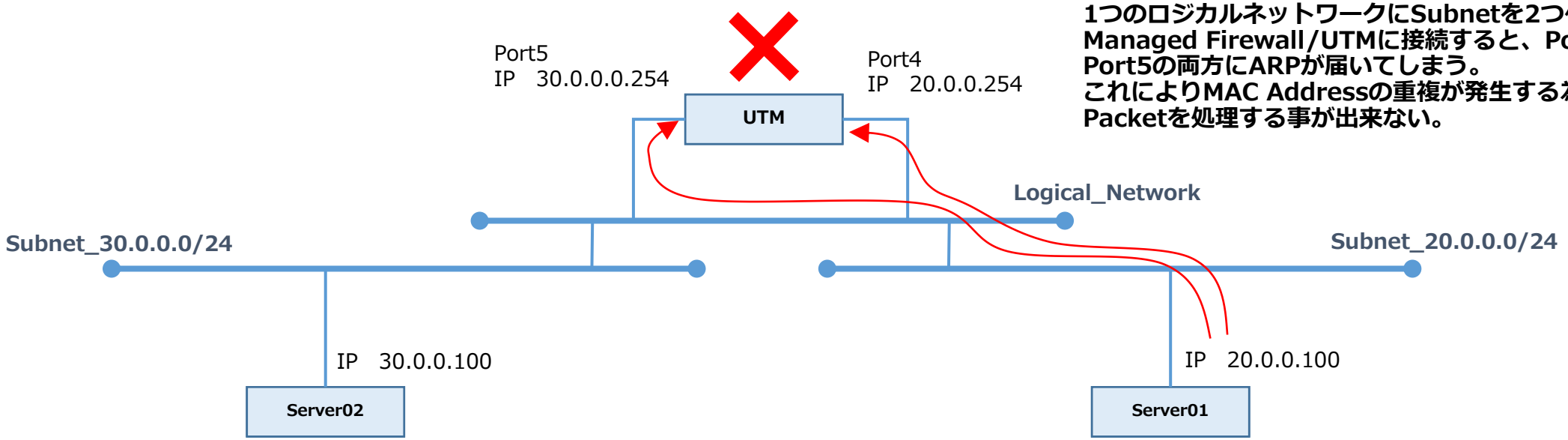


Managed Firewall/UTMからみて、同一のVRRP ID(同一のMAC Address【00:00:5e:00:01:01】)が、自分自身のPort4とPort5が同一、かつPort4とPort5の先に存在する。その為、Managed Firewall/UTMは正常にPacketを処理する事が出来ない。

・自分自身で重複するMAC Addressを持ってはいけない
・隣接する機器にて、重複するMAC Addressを持ってはいけない

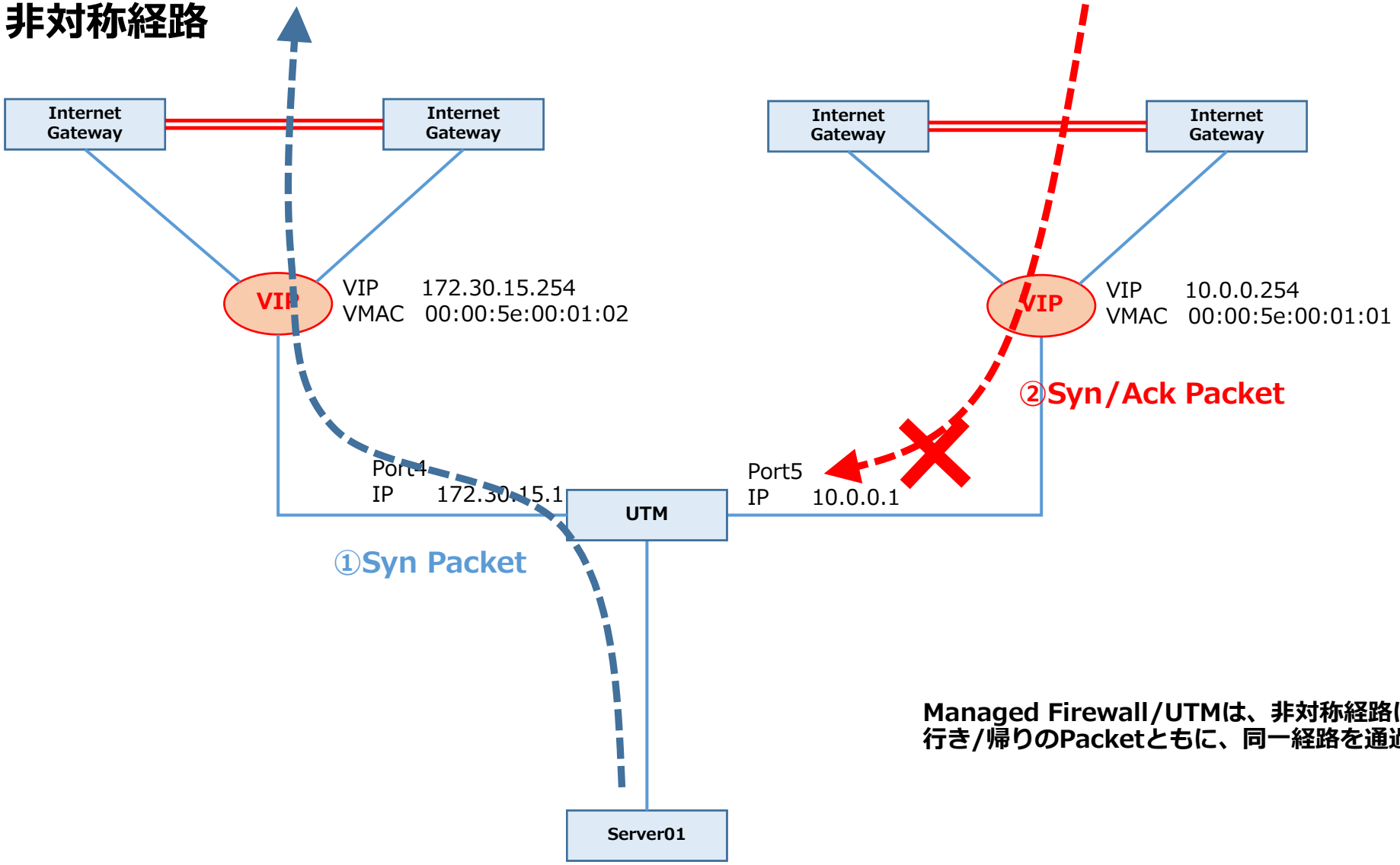
ロジカルネットワーク上の他メニュー/持ち込み製品などのVRRP IDは、本メニューに設定するVRRP IDとも重複しないように、11以外の値で、1、2のように別々の値を設定してください。

MAC Address重複



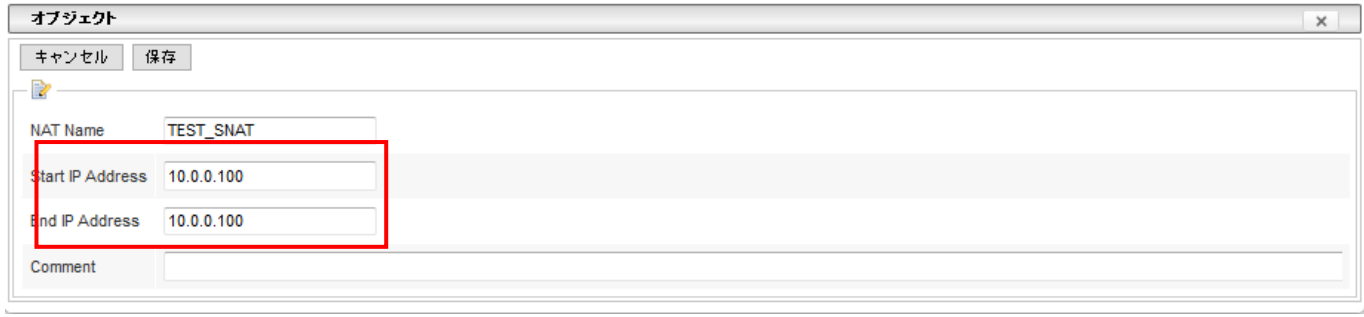
1つのロジカルネットワークにSubnetを2つ作成し、Managed Firewall/UTMに接続すると、Port4とPort5の両方にARPが届いてしまう。
これによりMAC Addressの重複が発生する為、正常にPacketを処理する事が出来ない。

非対称経路



Managed Firewall/UTMは、非対称経路に対応しておりません。
行き/帰りのPacketともに、同一経路を通過する様設定願います。

Source NAT Objectの制限

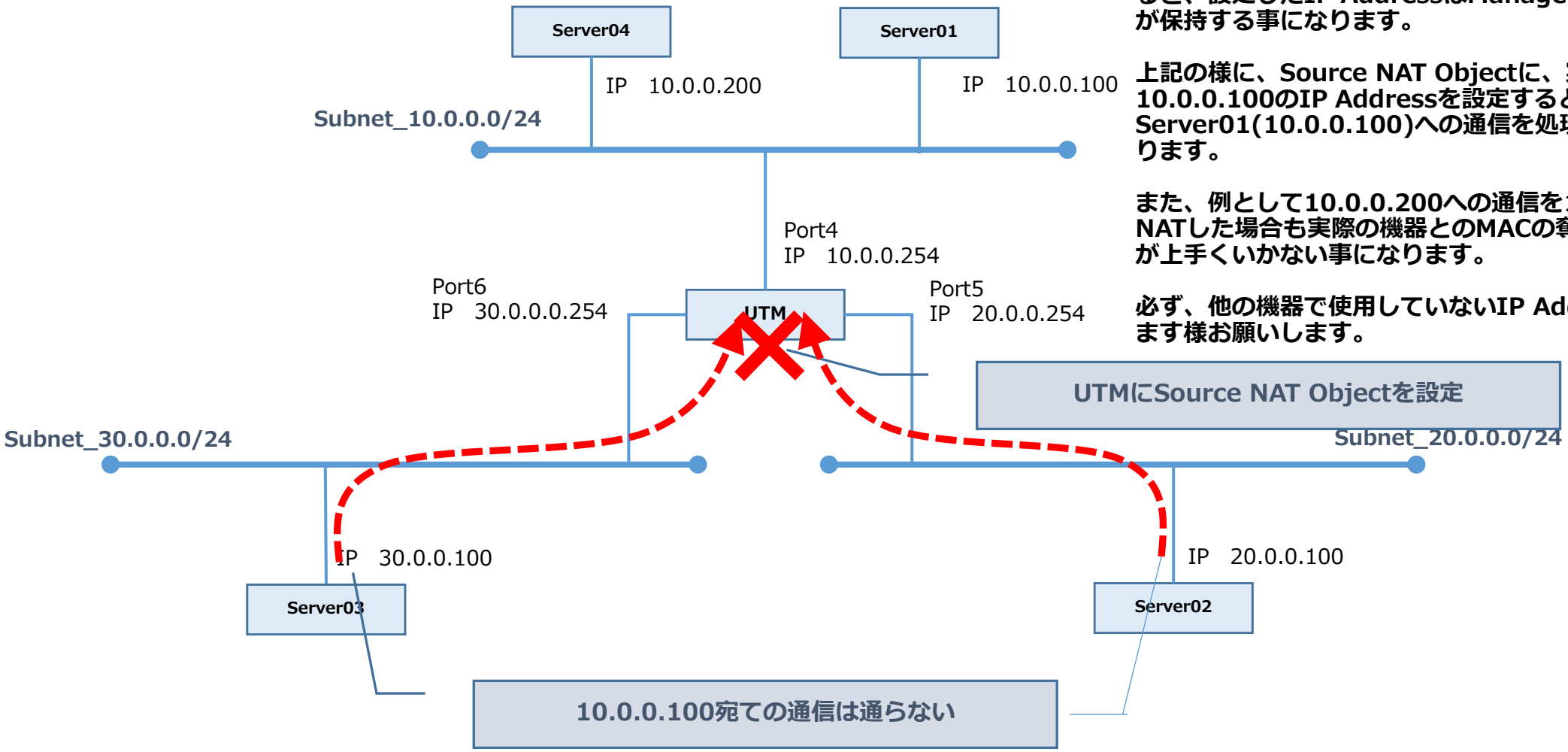


Managed Firewall/UTMに、Source NAT Objectを作成すると、設定したIP AddressはManaged Firewall/UTM自身が保持する事になります。

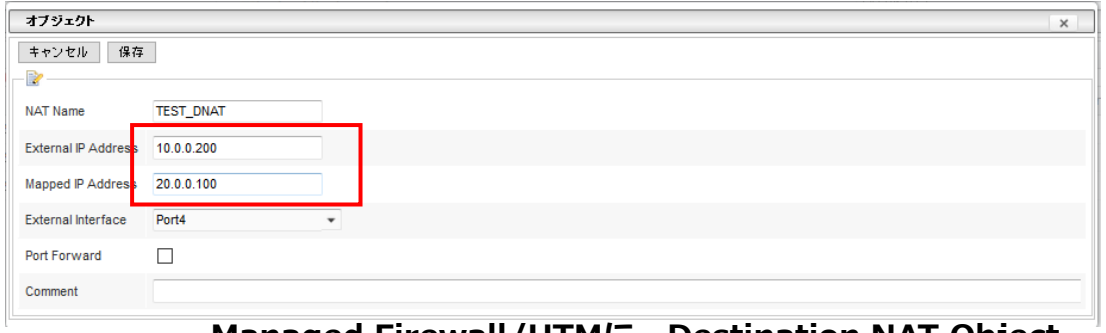
上記の様に、Source NAT Objectに、実際に存在する10.0.0.100のIP Addressを設定すると、Server01(10.0.0.100)への通信を処理する事は出来なくなります。

また、例として10.0.0.200への通信を10.0.0.100のIPにNATした場合も実際の機器とのMACの奪い合いになり、通信が上手くいかない事になります。

必ず、他の機器で使用していないIP Addressを設定して頂きます様お願いします。



Destination NAT Objectの制限

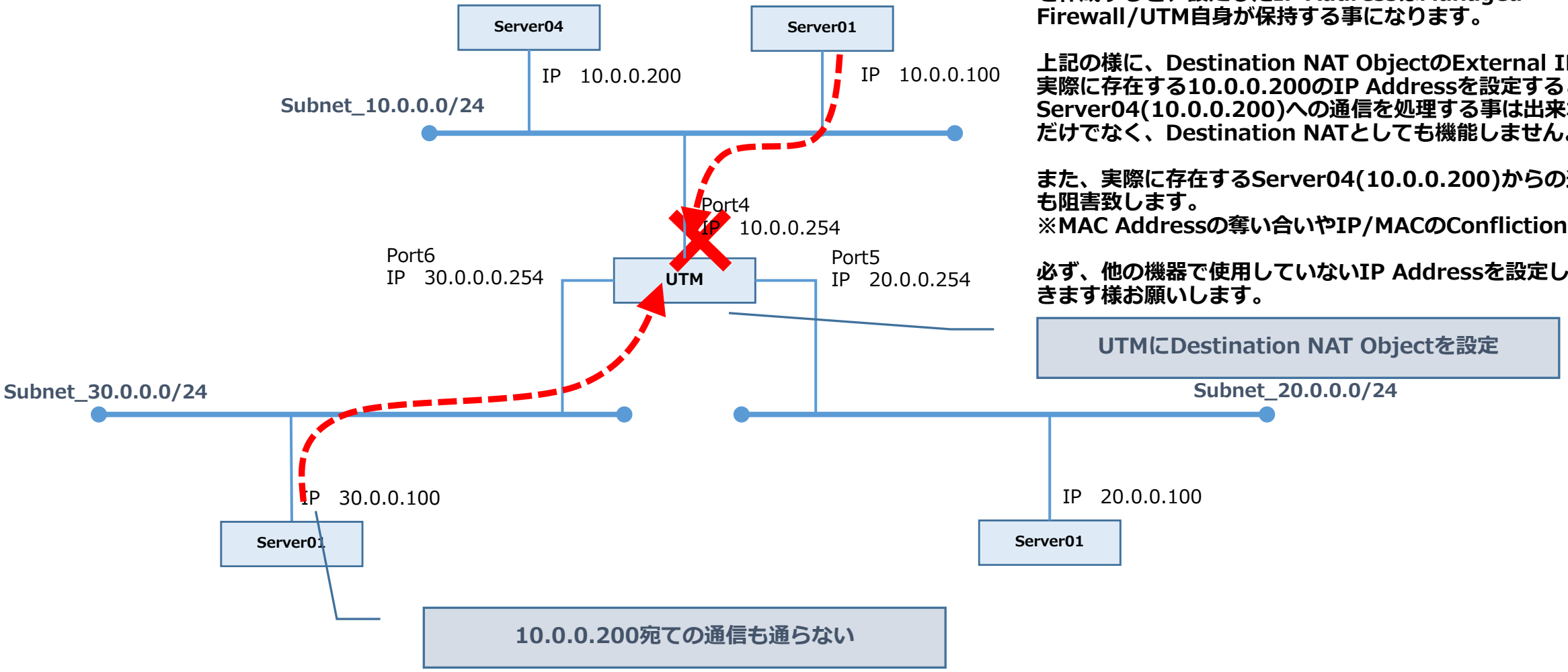


Managed Firewall/UTMに、Destination NAT Objectを作成すると、設定したIP AddressはManaged Firewall/UTM自身が保持する事になります。

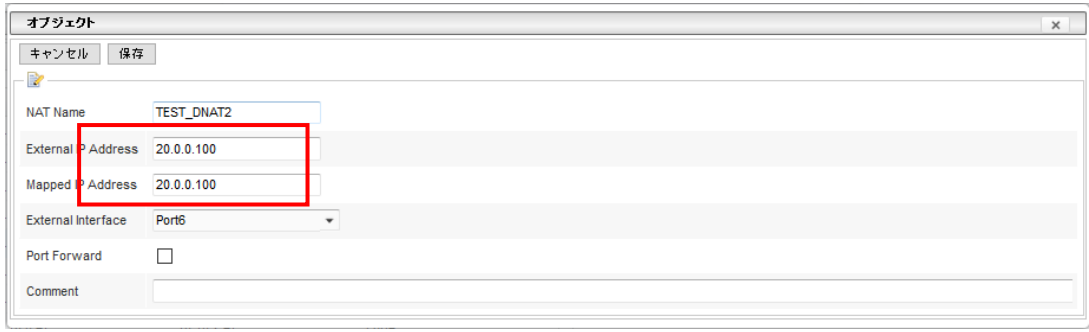
上記の様に、Destination NAT ObjectのExternal IPに、実際に存在する10.0.0.200のIP Addressを設定すると、Server04(10.0.0.200)への通信を処理する事は出来ないだけでなく、Destination NATとしても機能しません。

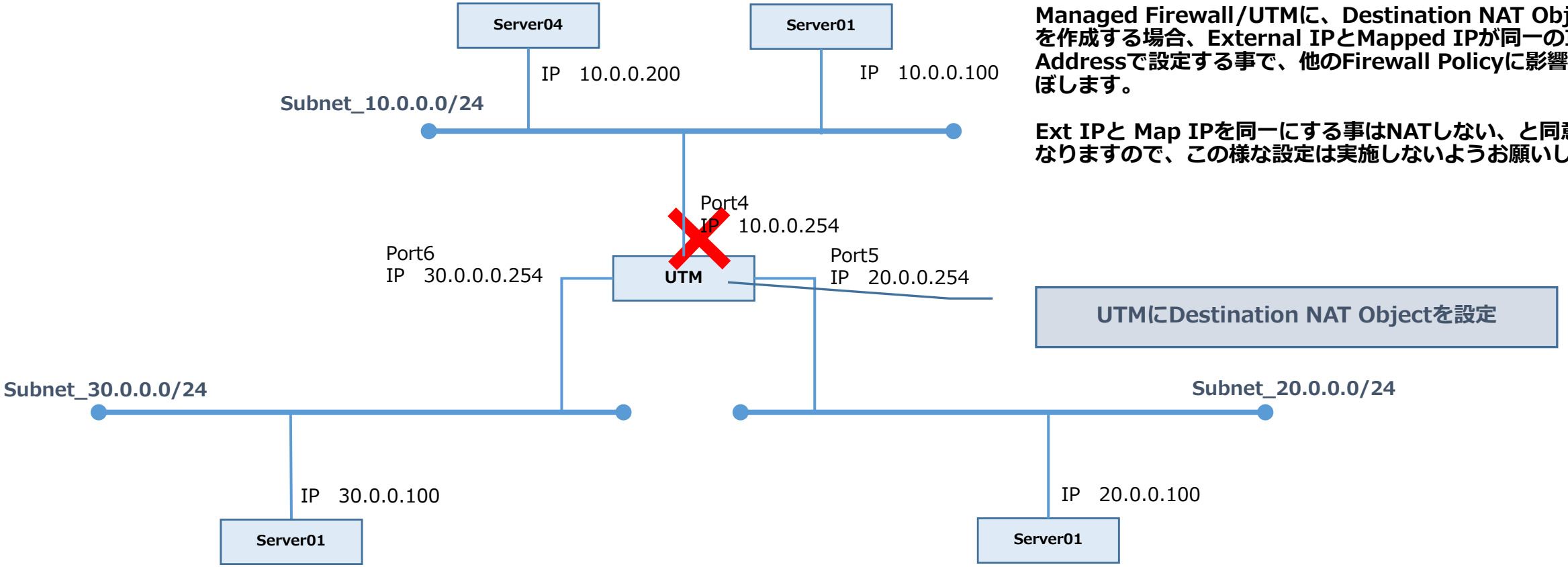
また、実際に存在するServer04(10.0.0.200)からの通信も阻害致します。
※MAC Addressの奪い合いやIP/MACのConfliction

必ず、他の機器で使用していないIP Addressを設定して頂きます様お願いします。



Destination NAT Objectの制限2



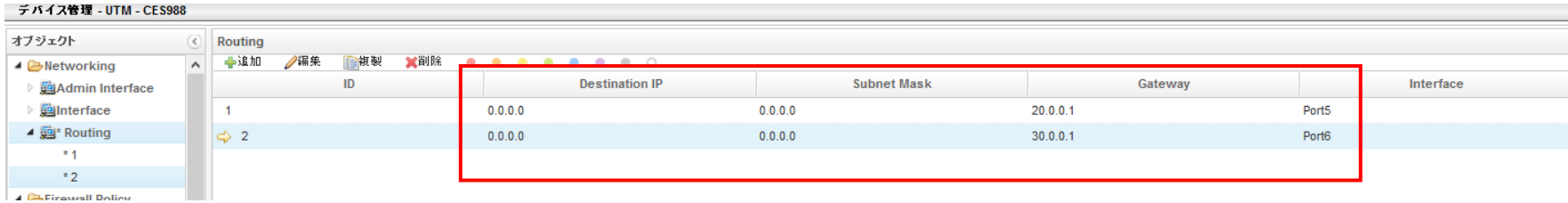


Managed Firewall/UTMに、Destination NAT Objectを作成する場合、External IPとMapped IPが同一のIP Addressで設定する事で、他のFirewall Policyに影響を及ぼします。

Ext IPと Map IPを同一にする事はNATしない、と同意になりますので、この様な設定は実施しないようお願いします。

UTMにDestination NAT Objectを設定

Routingの制限

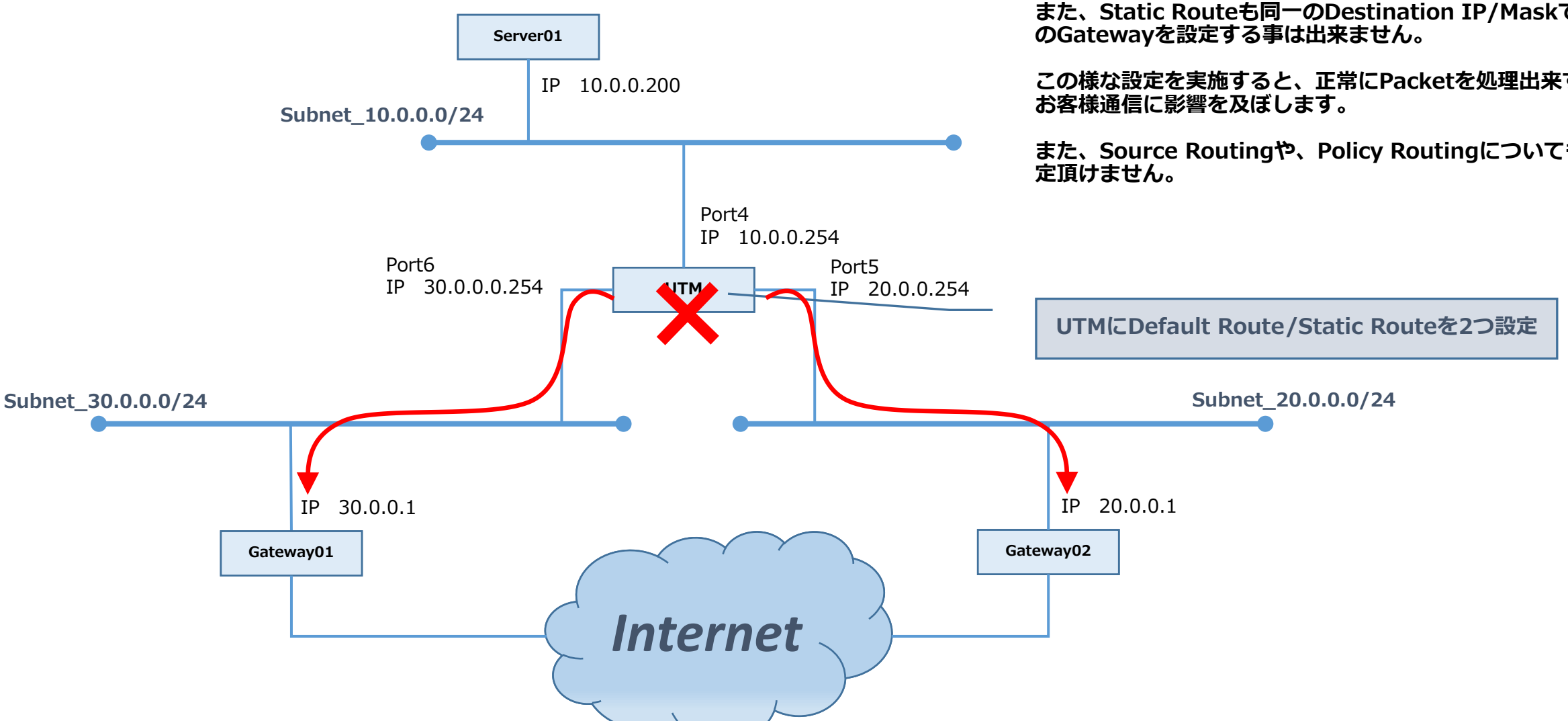


Managed Firewall/UTMに、2つ(以上)のDefault Routeを設定する事は出来ません。

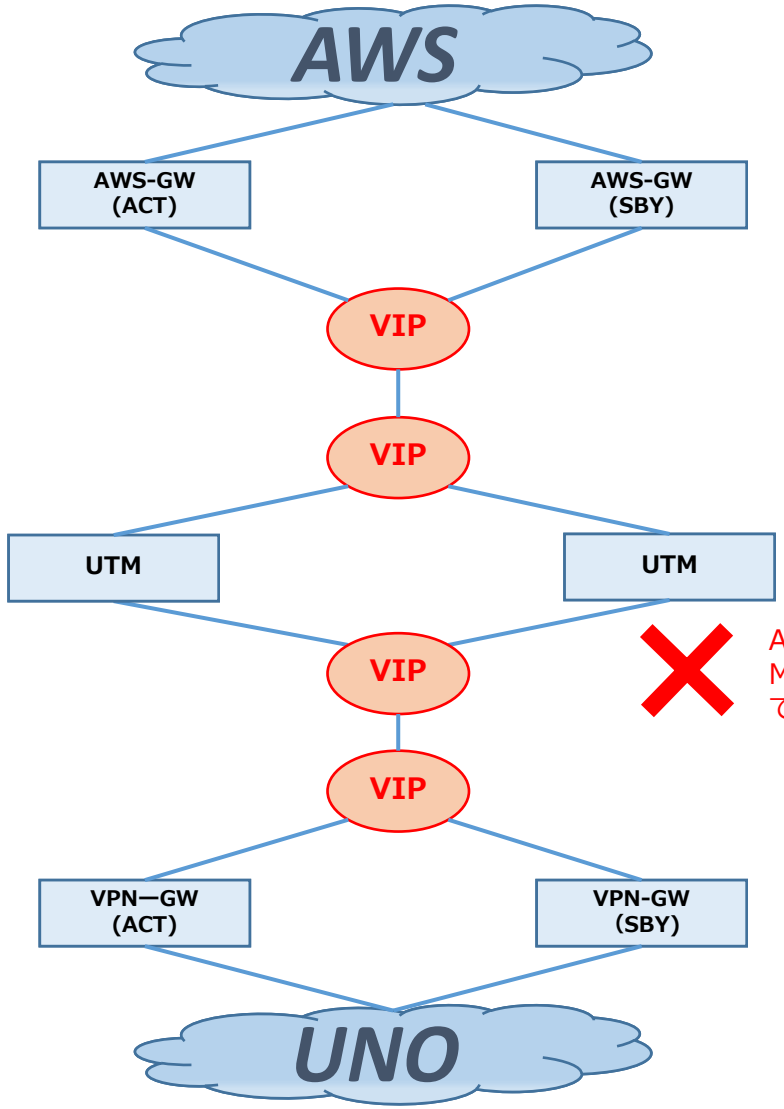
また、Static Routeも同一のDestination IP/Maskで別のGatewayを設定する事は出来ません。

この様な設定を実施すると、正常にPacketを処理出来ず、お客様通信に影響を及ぼします。

また、Source Routingや、Policy Routingについても設定頂けません。



AWSゲートウェイ、VPNゲートウェイを含む構成における制限



AWS-GWとVPN-GWを1台(1式)の
Managed Firewall/UTMで接続する構成
では動作不可。

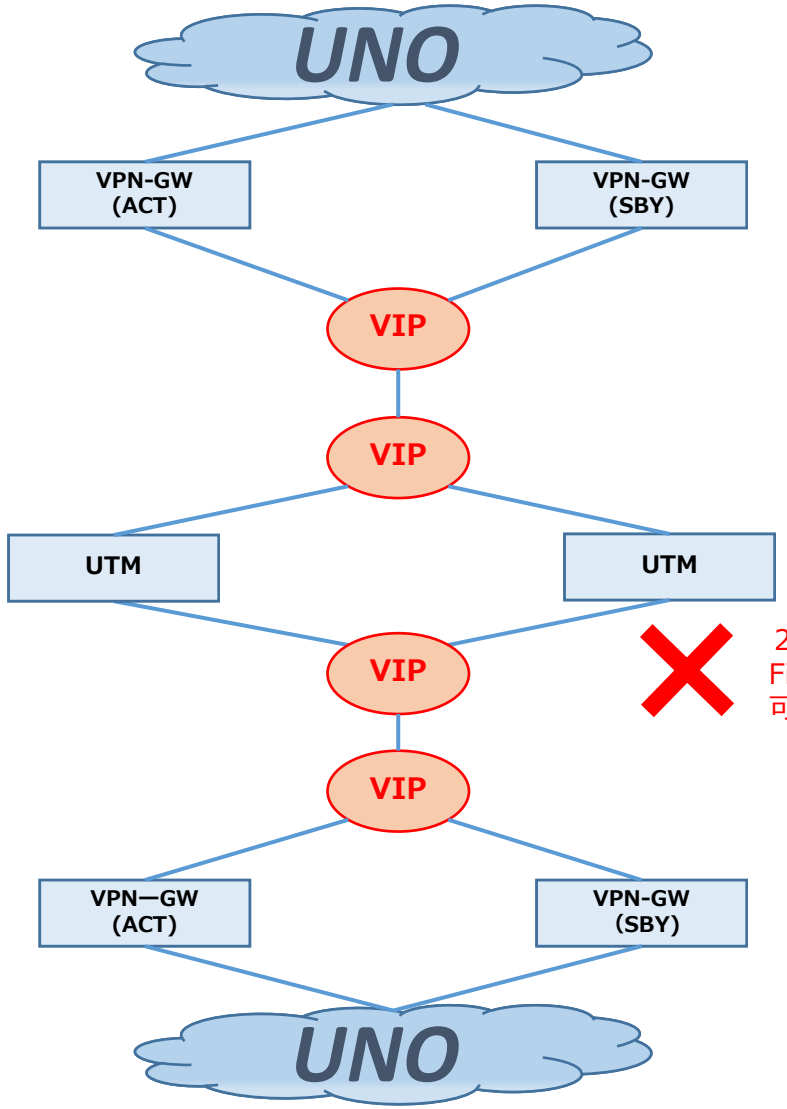
AWSゲートウェイやVPNゲートウェイを、1台のManaged FirewallもしくはManaged UTM経由で接続する構成では動作しません。

Managed FWもしくはManaged UTMとL3ノードを多段構成にしてください。

一部のアプライアンスでは、隣接するセグメントに重複したMACアドレスが存在する場合に通信が出来ないことが確認されています。

当該構成についてご不明な点がございましたら、弊社営業担当までご連絡ください。

２つのVPNゲートウェイを含む構成における制限



２つのVPN-GWを1台(1式)のManaged Firewall/UTMで接続する構成では動作不可。

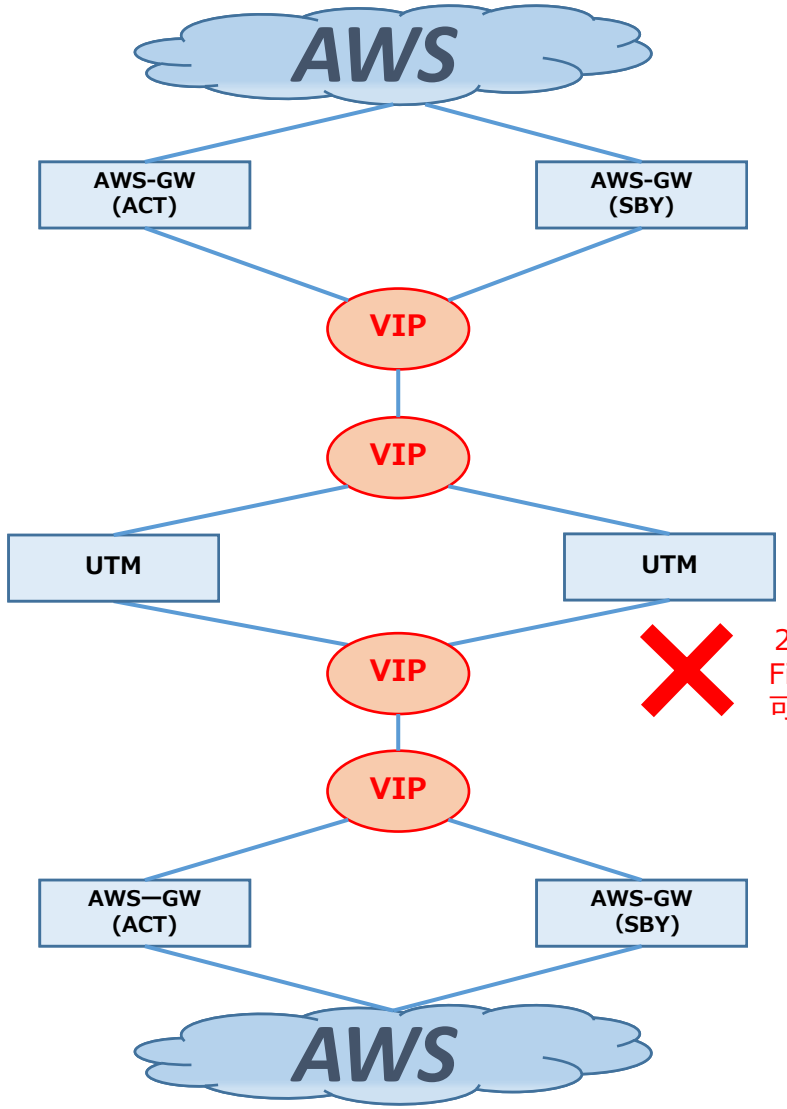
２つのVPNゲートウェイを、1台のManaged FirewallもしくはManaged UTM経由で接続する構成では動作しません。

Managed FWもしくはManaged UTMとL3ノードを多段構成にしてください。

一部のアプライアンスでは、隣接するセグメントに重複したMACアドレスが存在する場合に通信が出来ないことが確認されています。

当該構成についてご不明な点がございましたら、弊社営業担当までご連絡ください。

２つのAWSゲートウェイを含む構成における制限



２つのAWS-GWを1台(1式)のManaged Firewall/UTMで接続する構成では動作不可。

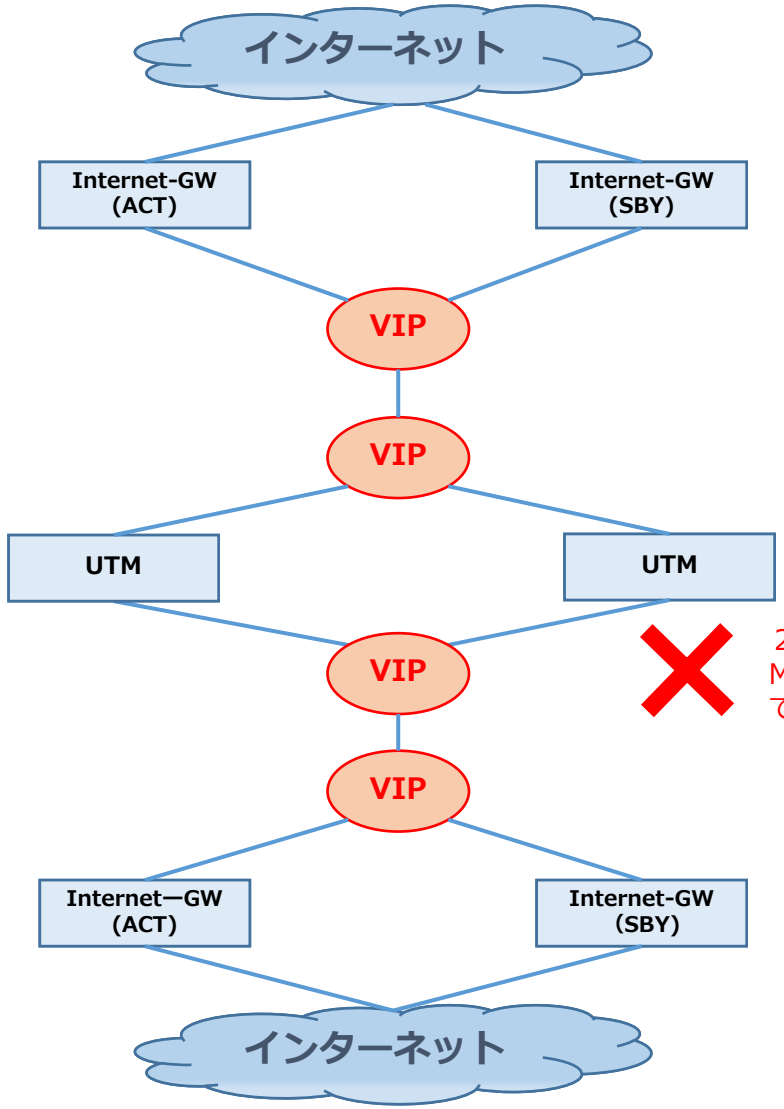
２つのAWSゲートウェイを、1台のManaged FirewallもしくはManaged UTM経由で接続する構成では動作しません。

Managed FWもしくはManaged UTMとL3ノードを多段構成にしてください。

一部のアプライアンスでは、隣接するセグメントに重複したMACアドレスが存在する場合に通信が出来ないことが確認されています。

当該構成についてご不明な点がございましたら、弊社営業担当までご連絡ください。

２つのインターネットゲートウェイを含む構成における制限



２つのInternet-GWを1台(1式)の
Managed Firewall/UTMで接続する構成
では動作不可。

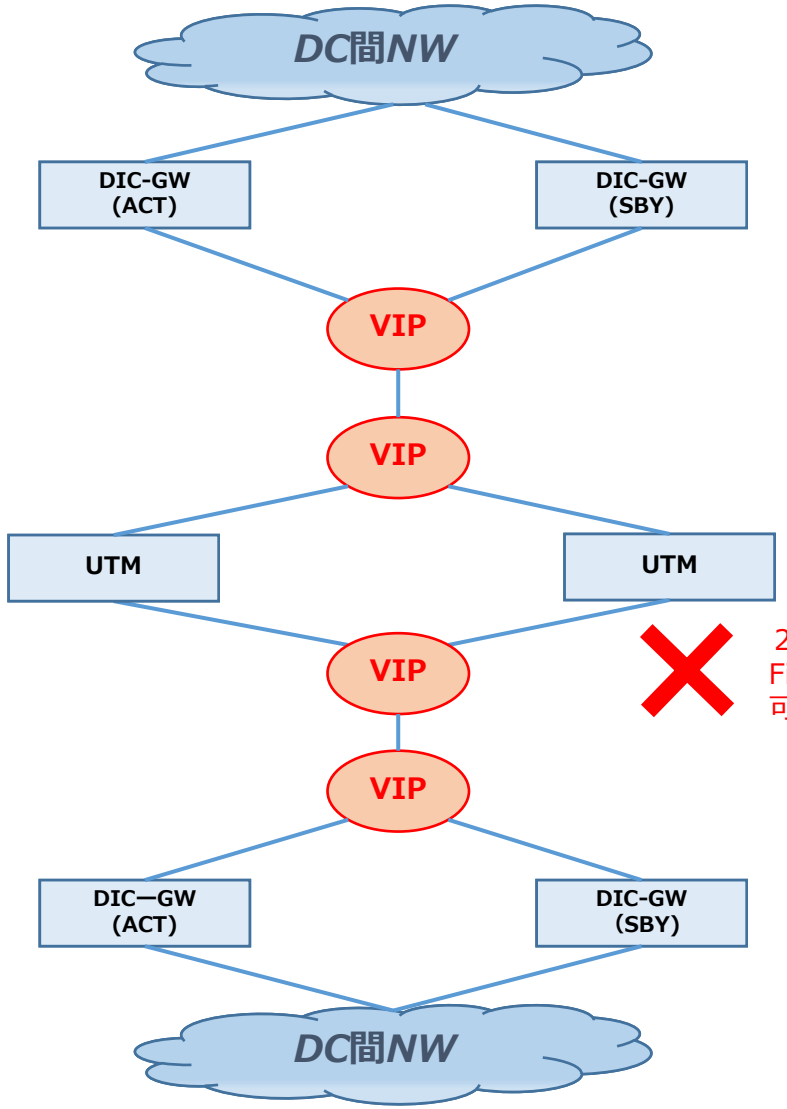
２つのInternetゲートウェイを、1台のManaged Firewallもしくは Managed UTM経由で接続する構成では動作しません。

Managed FWもしくはManaged UTMとL3ノードを多段構成にしてください。

一部のアプライアンスでは、隣接するセグメントに重複したMACアドレスが存在する場合に通信が出来ないことが確認されています。

当該構成についてご不明な点がございましたら、弊社営業担当までご連絡ください。

２つのDC間接続ゲートウェイを含む構成における制限



２つのDIC-GWを1台(1式)のManaged Firewall/UTMで接続する構成では動作不可。

２つのDC間接続ゲートウェイを、1台のManaged FirewallもしくはManaged UTM経由で接続する構成では動作しません。

Managed FWもしくはManaged UTMとL3ノードを多段構成にしてください。

一部のアプライアンスでは、隣接するセグメントに重複したMACアドレスが存在する場合に通信が出来ないことが確認されています。

当該構成についてご不明な点がございましたら、弊社営業担当までご連絡ください。