How To | Allow Public and Private Address Access to Servers at a Service Provider Client Site

Introduction

This document contains configuration examples and guidelines for a situation that uses firewall and enhanced NAT where you need to make a server's registered public address accessible from hosts on the firewall's private interface. It also addresses several common security requirements when deploying Allied Telesis switches or routers into shared user / access level environments.

What information will you find in this document?

This document is divided into the following sections:

Which products and software version does this information apply to?

The information provided in this document applies to:

Products:

This is a multiple solution document. Some components are limited to certain products (for example Private VLAN), while other components are more widely available (firewall with DMZ solution for example).

Note: *The diagrams and configuration examples in this document assume that the product being used is the AT-8824 switch. However, a number of different Allied Telesis routers or switches could be used in this application.*

Software version:

- 2.7.3 and above

Access to server public addresses

When a natting firewall provides public access to a server that sits on the private side of the firewall, it is often desirable that other hosts on the private side of the firewall be able to access the server via the publically available address.

For example, this means that there is no need to keep separate DNS records for the server - one record to provide for the private address hosts on the private side of the firewall, and another record to provide the server's public address to hosts on the public side of the firewall. There need simply be just one DNS entry for the server, that provides the public address.

Also, it means that users who sometimes connect their laptops to the private LAN, and access the server from there, and who at other times access the server from public locations, can always use the same address to access the server.

In this how-to note we provide three separate solutions to this requirement, using Allied Telesis routers, and is applicable to any network that uses Network Address Translation (NAT) and the security services of the Allied Telesis Firewall.

An example scenario is a small Multi Dwelling Unit (MDU) in which a few residential and / or SOHO clients are provided Internet connectivity via a Layer 3 switch or router.

The router / switch provides security in the form of a firewall, and performs NAT, so that a private address range can be used by the clients. In addition to Internet access from a private address, the service provider also wishes to give some of the clients the ability to host one or more servers with public IP addresses. These servers need to be able to be accessed from the external Internet, and from the local clients.

The three ways in which the network could be designed to support this combination of requirements are:

- host the servers on a separate DMZ VLAN
- use a firewall double NAT rule
- configure NAT to use a different public IP address than the IP address configured on the public interface of the firewall

Host the servers on a separate DMZ VLAN

The DMZ (Demilitarized Zone) solution is much more common. DMZ is a small sub-network that sits between a trusted internal network such as a corporate private LAN or shared access level users and an untrusted external network such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

In this case, public access to and from the DMZ is controlled by two firewall policies. This does have the slight disadvantage that it adds some complexity to the configuration, and management of the firewall. However, it does allow full access to the DMZ server(s) from private or public hosts via the publicly registered ip address(es).

Use a firewall double NAT rule

The Single Firewall Policy and Double NATing Firewall Rules solution has the limitation that it only opens up access to the public address of the server(s) for certain private hosts on a one by one basis. Therefore, in most situations it is impractical because all the private hosts would actually want this server access facility.

Use a different global IP on the NAT configuration

The third solution, using a different global IP on the NAT configuration, also has advantages and disadvantages.

One strong advantage is it is a Single Firewall Policy solution, so it is easier to understand than a Dual Firewall Policy solution.

The disadvantage is that the solution requires the Firewall Gateway Router to have at least three public Internet addresses registered and routed from the Internet to it. So, a small subnet of public addresses will need to be allocated to the site, not just a single public IP.

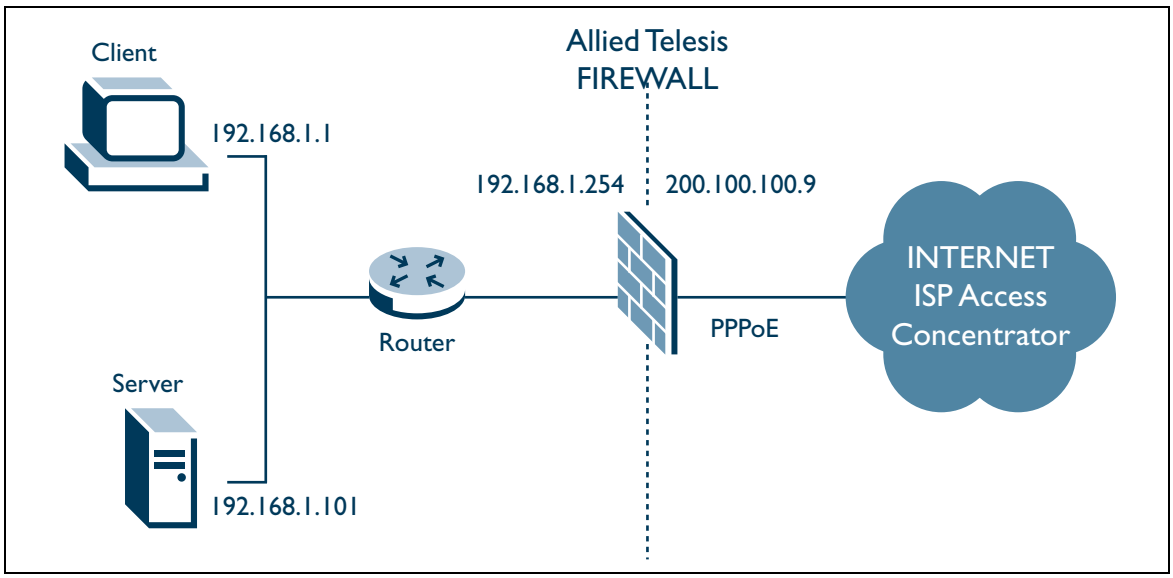
Another disadvantage is that traffic from LAN host to the public address of the server will in fact need to route via the ISP's Access Concentrator and be routed back again. Normally this will simply work because the ISP will have a route to our gateway for all those registered addresses. But, in unusual cases, some ISPs would block a packet that wants to "bounce back" from whence it came.

A prerequisite of this solution is that the gblip addresses for the firewall interface NAT statement and the firewall rule are not the address OWNED by the WAN interface - therefore they are proxy addresses, and when used as a destination address in the packet, will be routed out and returned via the ISP Access Concentrator.

Solution configuration

For a network where the web client is 192.168.1.1, and the web server is 192.168.1.101. The client is connecting to destination 200.100.100.11, which is the proxy Internet address of the web server - defined using gblip parameter in the Firewall rule.

This solution includes a PPPoE interface for Internet access



The whole subnet 200.100.100.8/255.255.255.248 has been allocated to the site where the Allied Telesis firewall is located. So the ISP will route ANY addresses in that subnet to the Allied Telesis firewall.

```
# System configuration
set system name="Single Policy Firewall and Server Access"

# PPP configuration
create ppp=0 over=eth0-any
set ppp=0 bap=off iprequest=on username="internet1" password="internet1"
set ppp=0 over=eth0-any lqr=off echo=10

# IP configuration
enable ip
enable ip remote

# The solution needs 3 Internet addresses
## The WAN interface address may be dynamically assigned or manually configured.
## To avoid Firewall spoof attack being declared it is recommended to make the address assigned to the public interface be host specific.  We can rely on the gblip addresses of the Firewall rules and NAT relationships to setup additional "proxy" public addresses.

add ip int=ppp0 ip=200.100.100.9 mask=255.255.255.255
# If the interface is to be dynamically assigned use as below, but if you use this you should ideally ensure that a host specific mask is assigned to avoid spoof attacks:
# add ip int=ppp0 ip=0.0.0.0 mask=0.0.0.0

add ip int=vlan1 ip=192.168.1.254
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

# Firewall configuration
enable firewall
create firewall policy="net"
enable firewall policy="net" log=deny
enable firewall policy="net" icmp_f=all
add firewall policy="net" int=vlan1 type=private
add firewall policy="net" int=ppp0 type=public


# This is Internet address 2, a proxy address. The key to the solution is that the address configured as the global IP on the net definition is different to the IP address configured on the PPP0 interface (the public interface of the firewall).
add firewall poli="net" nat=enhanced int=vlan1 gblin=ppp0 gblip=200.100.100.10

# This is Internet address 3, a proxy address.
## Because the rule needs to quote an gblip address not owned by the WAN interface and different to the gblip of the enhanced nat interface relationship - then this rule must be an action=nat rather than action=allow.
The gblip IP configured in this rule is the public IP address via which the server will be accessed

add firewall poli="net" rule=1 act=nat  int=ppp0 protocol=tcp po=80
ip=192.168.1.101 gblip=200.100.100.11 gblport=80

# HTTP configuration
disable http server
# GUI configuration
disable gui
```

To see how the solution works, consider a TCP session from a host on the private LAN to the public IP of the server.

The resultant packet sequence for a TCP session setup, would proceed as follows:

Action	Source IP	Destination IP
The host sends a TCP SYN	192.168.1.1	200.100.100.11
The firewall receives the packet, creates a NAT session, and changes the source IP of the packet to 200.100.100.10		
The packet will go out to the ISP and be bounced back. The firewall sees this packet as belonging to a NEW incoming TCP session. If the source IP address of the packet had been the router's OWN public address, it would have dropped the packet, but because the IP address is not the router's OWN IP, it passes the packet to NAT for processing.		
NAT creates a new incoming session for the packet.		
It sees that the destination IP address on the packet is the public address of the server. So, following the instructions of firewall rule 1, it changes the destination IP address to the private address of the server.	200.100.100.10	192.168.1.101
The packet is then delivered to the server.		
The server replies with a SYN ACK		
The SYN ACK is from the server's private IP to the source IP of the SYN packet.	192.168.1.101	200.100.100.10
When the packet arrives at the firewall, it sees this as a packet in the second (incoming) session that it created. It changes the source IP of the packet to the server's public IP and sends it out the ISP.		
The ISP sees that the dest IP of the packet is in the 200.100.100.8/29 subnet, so it bounces back to the firewall. The firewall sees this packet as belonging to the first, outgong session it created. It changes the Dest IP pf the packet to the host's IP address.	200.100.100.11	192.168.1.1
The SYN ACK is then delivered to the host.		
The first packet exchange of the TCP session is then complete.		

The rest of the TCP session continues in the same way, with packets going out through the firewall, being natted by one NAT session, bouncing back from the ISP, and being natted by the other NAT session.

The command **show firewall session** would show two NAT sessions. In the output below, session ce31 is the first, outgoing, session, where the IP address 192.168.1.1 is natted to the global IP 200.100.100.10. The session eceb is the second, incoming session, where the public address of the server (200.100.100.11) is natted to the private address of the server (192.168.1.101).

```
Show  firewall session
 Policy : net
 Current Sessions
 ------------------------------------------------------------------------
 ce31 TCP      IP: 192.168.1.1:1425          Remote IP: 200.100.100.11:80
          Gbl IP: 200.100.100.10:52785   Gbl Remote IP: 200.100.100.11:80
      TCP state ........................... open
      Start time .......................... 16:24:58 07-Aug-2009
      Seconds to deletion ................. 6
 eceb TCP     IP: 192.168.1.101:80          Remote IP: 200.100.100.10:52785
          Gbl IP: 200.100.100.11:80    Gbl Remote IP: 200.100.100.10:52785
      TCP state ........................... open
      Start time .......................... 16:24:58 07-Aug-2009
      Seconds to deletion ................. 6

 ------------------------------------------------------------------------
```

User separation

Shared user / access level switch solutions require security between the users even if they are on the same layer 2 VLAN. This can be achieved by creating private VLANs where the ports on the VLAN cannot access each other but can only access the defined uplink, or be layer 3 routed.

So, both solutions presented in this note must incorporate the requirement that the MDU clients are attached to a private VLAN.

Note: *Because this How To note uses a private VLAN with a firewall rather than an uplink, it means there can be no layer 2 wire-speed switching. All traffic will be layer 3 routed at CPU processing speed.*

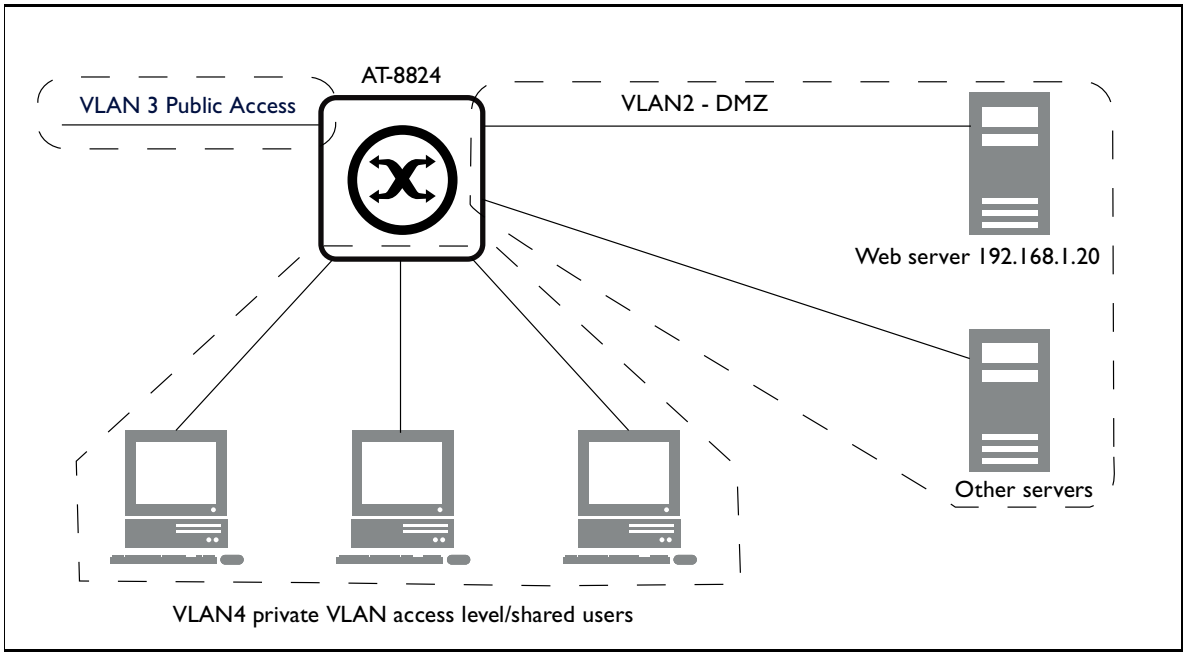
Step-by-step solutions

There are two step by step solutions:

- DMZ solution
- Firewall Double NATing solution

DMZ solution

This configuration provides the DMZ solution on an AT-8824 while utilising a private VLAN for access customers. (Some other AT routers and switches are also suitable for this firewall solution.) For this solution, both the DMZ and the access-level /shared users' VLAN are behind firewall NAT.



1. Create three VLANs:
   - VLAN 2 for the DMZ
   - VLAN 3 for the public Internet
   - VLAN 4 as a private VLAN

```
create vlan=DMZ vid=2
create vlan=public vid=3
```

VLAN 4 will be used for access-level /shared users', so it is created as a private VLAN. This will ensure that the ports of this VLAN cannot send traffic directly to each other. They must use an uplink or be layer 3 routed through the firewall:

```
create vlan=private_access vid=4 private
```

2. Add suitable ports to each VLAN:

```
add vlan=2 port=21-22
add vlan=3 port=23-24
add vlan=4 port=1-20
```

The bulk of the ports are devoted for the private VLAN for access-level /shared users. Ports 21 and 22 are used for the DMZ. Ports 23 and 24 are used for Public Internet connection.

3. Configure the IP. Some example addresses are given here for private addresses. Placeholders are shown for public addresses:

```
enable ip
add ip interface=vlan4 ip=192.168.0.1
add ip interface=vlan2 ip=192.168.1.1
add ip interface=vlan3 ip=< your public Internet address >
add ip route=0.0.0.0 mask=0.0.0.0 interface=vlan3 next=<your Internet gateway
   address>
```

4. You can also enable DNS Relay:

```
enable ip dnsrelay
add ip dns primary=< your public Internet DNS Server >
```

5. Create a firewall configuration for your private access-level /shared users' VLAN:

```
enable firewall
create firewall policy=LAN
enable firewall policy=LAN icmp_forwarding=ping
```

6. For this policy the access-level /shared users' VLAN is considered private:

```
add firewall policy=LAN interface=vlan4 type=private
add firewall policy=LAN interface=vlan3 type=public
add firewall policy=LAN interface=vlan2 type=public
```

7. Add an enhanced NAT definition for translation of private addresses when accessing the Internet:

```
add firewall policy=LAN nat=enhanced interface=vlan4 gblinterface=vlan3
```

8. Secondly create a firewall policy for your DMZ VLAN, which will cater for your public-access servers:

```
create firewall policy=DMZ
enable firewall policy=DMZ icmp_forwarding=ping
```

9. For this policy the DMZ VLAN is considered private:

```
add firewall policy=DMZ interface=vlan2 type=private
add firewall policy=DMZ interface=vlan3 type=public
add firewall policy=DMZ interface=vlan4 type=public
```

10. Add an enhanced NAT definition for translation of private addresses when accessing the Internet:

```
add firewall policy=DMZ nat=enhanced interface=vlan2 gblinterface=vlan3
```

11. Add a firewall allow rule to the DMZ policy to allow public access to a web server. This rule will also allow users on the access-level /shared users' VLAN to access the server via its public-registered IP address.

```
add firewall policy=DMZ rule=1 action=allow interface=vlan3 protocol=tcp
   port=80 ip=192.168.1.20 gblip=< your public Internet address > gblport=80
```

You can duplicate this rule for other services. You may use other gblp addresses and the firewall will automatically listen and make proxy-arp replies for this address on the public LAN (this can be verified with `sh fire arp`).

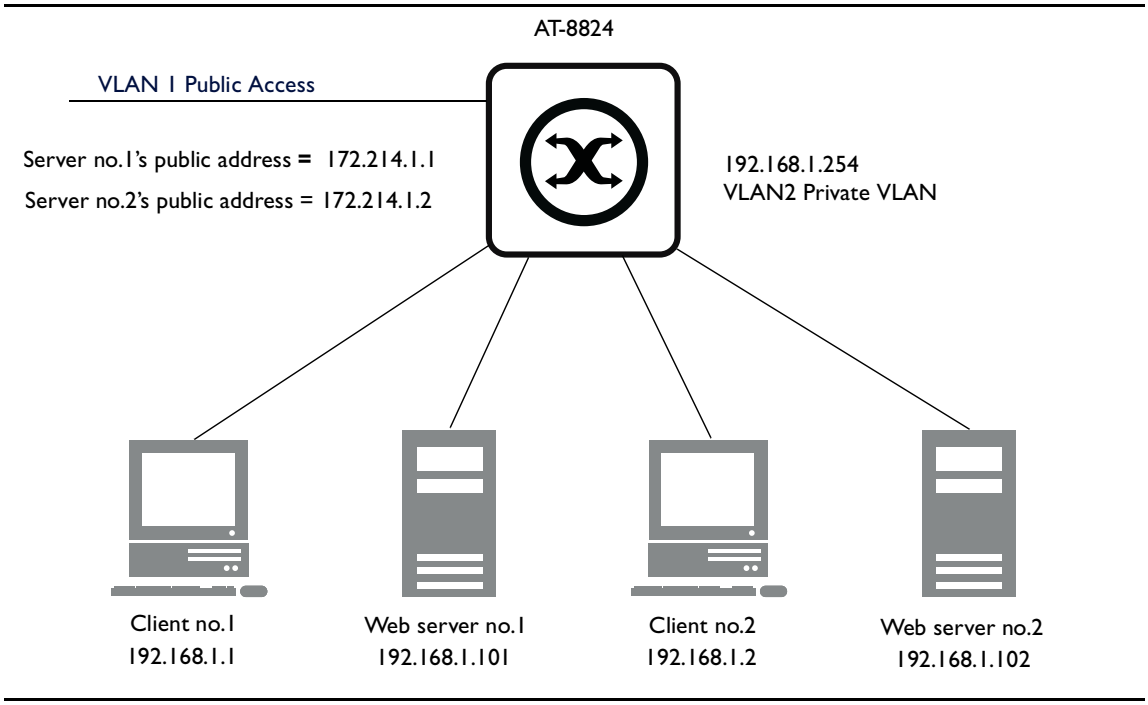
12. Disabling the switches' /routers' HTTP server will avoid any conflict with firewall allow rules for HTTP port 80:

```
disable http server
```

Firewall double NATing solution

This configuration does not need a DMZ VLAN. Instead the access-level users can also connect servers to their private VLAN ports.

The private VLAN is still behind a NATing firewall. If the users want to access the servers using their publicly registered addresses, then the firewall must include double-NAT type rules. However, these rules only allow a one-to-one mapping; one particular private address has to access the private server via its public address.



1. Create a private VLAN for access-level /shared users'. Private VLANs ensure that the ports of this VLAN cannot send traffic directly to each other. They must use an uplink or be layer 3 routed through the firewall:

```
create vlan=private vid=2 private
```

2. Add ports to the VLAN. The bulk of the ports are devoted for the access-level /shared users' VLAN. Ports 23 and 24 are left for the default VLAN 1, used for public Internet connection:

```
add vlan=2 port=1-22
```

3. Configure IP. Some example addresses are given here for private addresses. Placeholders are shown for public addresses:

```
enable ip
add ip interface=vlan1 ip=< your public Internet address >
add ip interface=vlan2 ip=192.168.1.254
add ip route=0.0.0.0 mask=0.0.0.0 interface=vlan1 next=< your Internet
gateway
   address >
```

4. Create a firewall configuration to protect your private access-level /shared users' VLAN:

```
enable firewall
create firewall policy=hostg
enable firewall policy=hostg icmp_forwarding=ping
```

5. In this double-nat example, VLAN 2 is private and VLAN 1 is public:

```
add firewall policy=hostg interface=vlan2 type=private
add firewall policy=hostg interface=vlan1 type=public
```

6. Add an enhanced NAT definition for translation of private addresses when accessing the Internet:

```
add firewall policy=hostg nat=enhanced interface=vlan2 gblinterface=vlan1
```

7. This example adds two firewall rules to allow public access to two web servers – 192.168.1.101 and 192.168.1.102. The firewall will automatically listen and make proxy-arp replies for the second public address – (for example, `< your public address 2 >`). Proxy arp can be verified with `sh fire arp`:

```
add firewall policy=hostg rule=1 action=nat interface=vlan1 protocol=tcp
   port=80 ip=192.168.1.1 gblip=< your public address 1 > gblport=80
add firewall policy=hostg rule=2 action=nat interface=vlan1 protocol=tcp
   port=80 ip=192.168.1.2 gblip=< your public address 2 > gblport=80
```

8. Two double NATing rules are now added. These allow access from nominated private LAN users to the web servers, by accessing the servers' registered public addresses:

```
add firewall policy=hostg rule=3 action=nat interface=vlan2 protocol=tcp
   port=80 ip=192.168.1.1 gblip=192.168.1.254 nattype=double
   gblremoteip=192.168.1.101
set firewall policy=hostg rule=3 remoteip=< your public address 1 >
add firewall policy=hostg rule=4 action=nat interface=vlan2 protocol=tcp
   port=80 ip=192.168.1.2 gblip=192.168.1.254 nattype=double
   gblremoteip=192.168.1.102
set firewall policy=hostg rule=4 remoteip=< your public address 2 >
#
# HTTP configuration
#
disable http server
```

In this case;

- The `ip` parameter is the initiating client.
- `gblip` is the common private-side-gateway that the private-side-servers and private-side-clients are using. So, this is the firewall's private interface VLAN2.
- `gblremoteip` is the private address of the server you want to connect to.
- `remoteip` is the public address that you want private clients to be able to connect to, which results in this address mapping to the private server defined by GBLRemote.

Therefore we could present the rules more generically in the following way;

```
add firewall policy=hostg rule=3 action=nat interface=vlan2 protocol=tcp
   port=80 ip=<initiating private-side-client> gblip=<private-side-gateway
   address> nattype=double gblremoteip=<private-server address>
set firewall policy=hostg rule=3 remoteip=< your public address 1 >
add firewall policy=hostg rule=4 action=nat interface=vlan2 protocol=tcp
port=80 ip=<initiating private-side-client> gblip=<private-side-gateway
   address> nattype=double gblremoteip=<private-server address>
set firewall policy=hostg ru=4 remoteip=< your public address 2 >
```

For more information see the How To Note titled: *How to configure some basic firewall and VPN scenarios*.

European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16085-00 REV B