

Zone	Interface				
	Name	Physical	VLAN	IP Address	Subnet Mask
Public			-	23.251.32.21	255.255.255.224
DMZ			-	192.168.1.1	255.255.255.0
Private			-	192.168.2.1	255.255.255.0

NAT Type	Host Name	Actual Address			Mapped Address		
		Interface	Address	Subnet Mask	Interface	Address	Subnet Mask
DNAT	*	private	192.168.2.0	255.255.255.0	public	23.251.32.21	255.255.255.255
SNAT	mail	dmz	192.168.1.11	255.255.255.255	public	23.251.32.22	255.255.255.255
SNAT	web	dmz	192.168.1.12	255.255.255.255	public	23.251.32.23	255.255.255.255

Destination	Next Hop	Interface	Metric
0.0.0.0	23.251.32.1	public	1
<i>*The router on the ISP's network is not explicitly stated in the problem Using the rule that gateways are the lowest value in an IP range it must be .1 as all of the given public interfaces are in the .0/27 range</i>			

Location of Rule		Address Match						Action	Description
		SRC			DST				
Interface	Direction	L3 IP	L4+ Protocol	Detail	L3 IP	L4+ Protocol	Detail		
public	in	*	*	*	192.168.1.11/32*	tcp	25	allow	Allow mail to mail server SNAT in dmz
public	in	*	*	*	192.168.1.11/32*	tcp	443	allow	Allow HTTPS to mail server SNAT in dmz
public	in	*	*	*	192.168.1.12/32*	tcp	80	allow	Allow HTTP to web server SNAT in dmz
public	in	*	*	*	192.168.1.12/32*	tcp	443	allow	Allow HTTPS to web server SNAT in dmz
public	in	*	*	*	192.168.1.8/29*	tcp	443	allow	Summarized HTTPS rule that replaces both of the rules in red - note that the extended network prefix is a /29 as that is the smallest way to get .11 and .12 together (10-13) - Ideally they should have been addressed as .10 and .11 or .12 and .13 whichi would have allowed a /31
public	in	*	*	*	*	*	*	deny	Drop all other traffic
dmz	in	*	*	*	54.6.59.2/32	udp	53	allow	Allow DMZ hosts to query DNS
dmz	in	*	*	*	192.168.0.0/16	*	*	deny	Scope the following destination wildcard
dmz	in	192.168.1.11/32	*	*	*	tcp	25	allow	Allow mail server to send SMTP
dmz	in	*	*	*	*	*	*	deny	drop all other traffic
private	in	*	*	*	192.168.1.11/32	tcp	25	allow	Allow SMTP to mail server
private	in	*	*	*	192.168.1.11/32	tcp	443	allow	Allow HTTPS to mail server
private	in	*	*	*	192.168.1.12/32	tcp	80	allow	Allow HTTP to web server
private	in	*	*	*	192.168.1.12/32	tcp	443	allow	Allow HTTPS to web server
private	in	*	*	*	192.168.1.8/29	tcp	443	allow	Summarized rule that can replace the two above red rules
private	in	*	*	*	192.168.1.12/32	tcp	137	allow	Allow SMB to web server
private	in	*	*	*	192.168.1.12/32	tcp	139	allow	Allow SMB to web server
private	in	*	*	*	192.168.1.12/32	tcp	80	allow	Allow HTTP to DMZ web server
private	in	*	*	*	192.168.1.0/24	tcp	22	allow	Allow SSH to all DMZ servers
private	in	*	*	*	192.168.1.0/24	*	*	deny	Drop all other traffic to DMZ
private	in	192.168.2.2/32	*	*	54.6.59.2/32	udp	53	allow	Allow internal DNS server to query DNS
private	in	192.168.2.2/32	*	*	54.6.59.2/32	udp	123	allow	Allow internal NTP server to query NTP
private	in	*	*	*	*	tcp	80	allow	Allow HTTP to anything on the Internet
private	in	*	*	*	*	tcp	443	allow	Allow HTTPS to anything on the Internet
private	in	*	*	*	*	*	*	deny	drop all other traffic