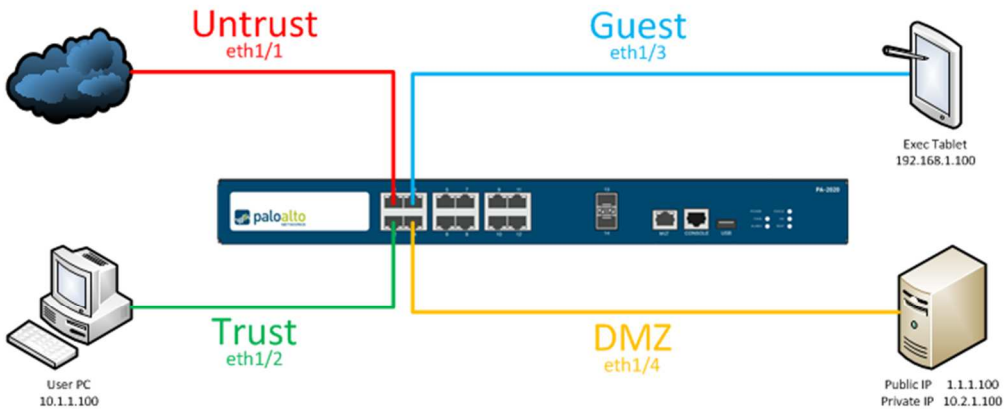
U-Turn NAT Example Configuration

03/2013

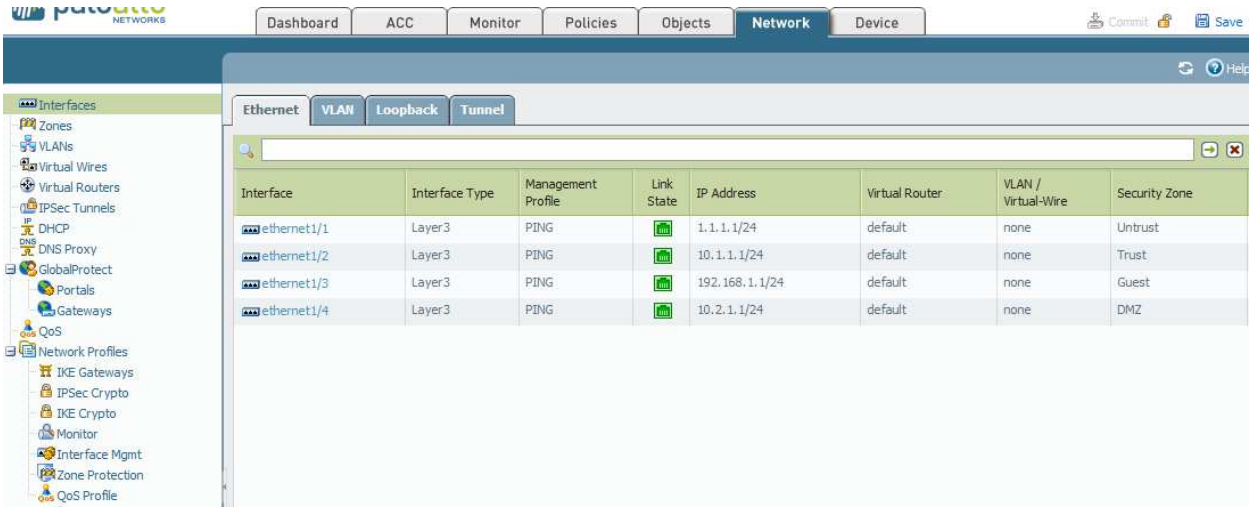
If services located on devices in separate zones must communicate using external IP addresses, U-Turn NATs must be configured.

In the below example we have 4 zones: Untrust which is the external feed from the Internet, the Trust zone is where the internal corporate network lives, the Guest zone is for employee smart phones/tablets & guest users, and DMZ which is where servers located. The webserver has a private address of 10.2.1.100 that is translated to 1.1.1.100, so that it can be accessed externally via the Internet. For reasons beyond IT's control, internal users and guest users must also access this webserver via its public address.



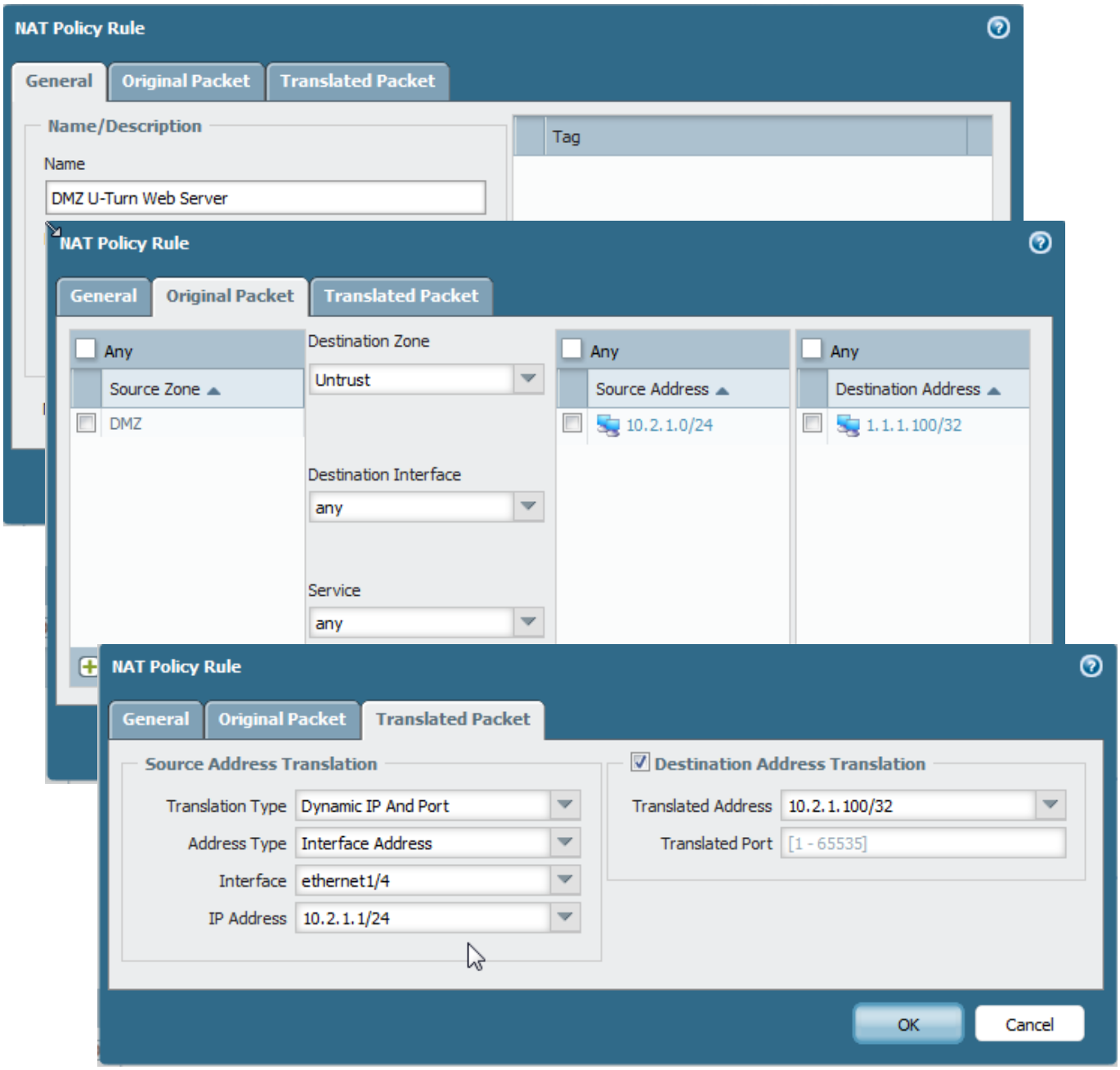
Untrust	eth1/1	1.1.1.1/24
Trust	eth1/2	10.1.1.1/24
Guest	eth1/3	192.168.1.1/24
DMZ	eth1/4	10.2.1.1/24

Interface layout:

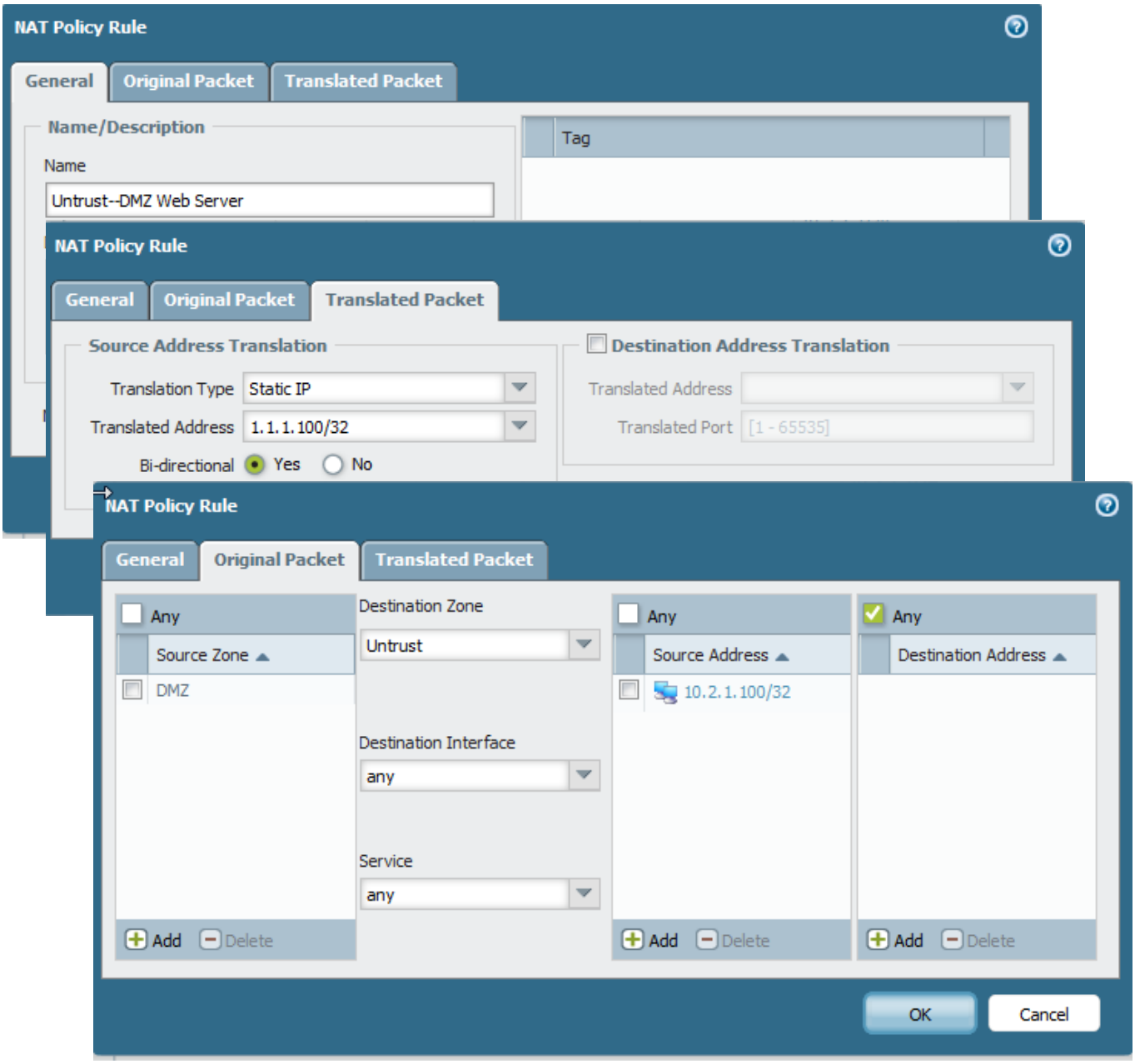


NAT Policies:

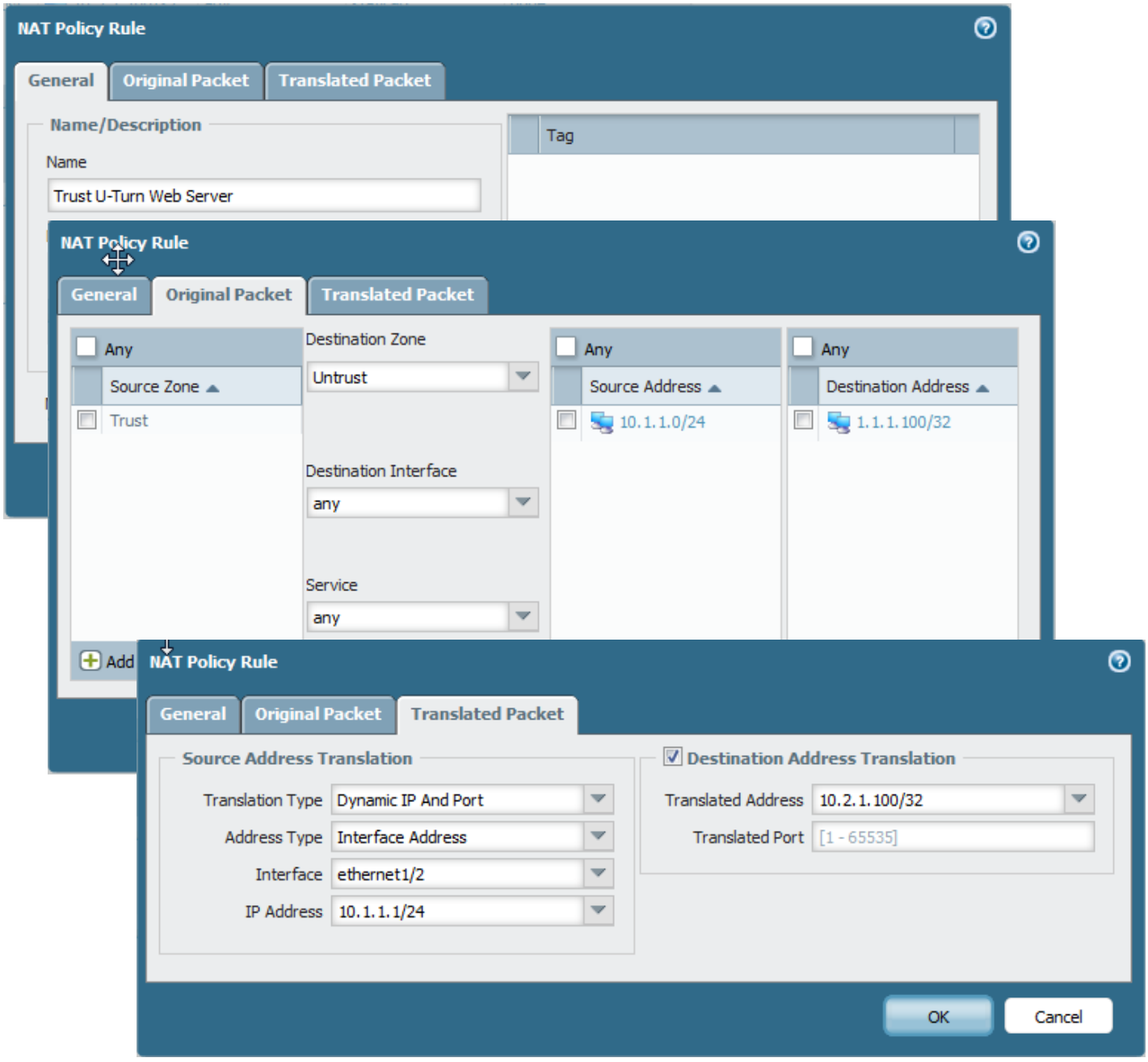
This rule translates traffic from the DMZ zone bound for the public IP address of the web server in the DMZ zone. The destination address of 1.1.1.100 is translated to 10.2.1.100, and the source address is translated to the IP address of interface ethernet1/3. NAT policies are processed in a top-down fashion. The ordering of these policies is import. Any U-Turn policies that have the same source and destination zones, must be placed before the one-to-one NAT policy for the destination server.



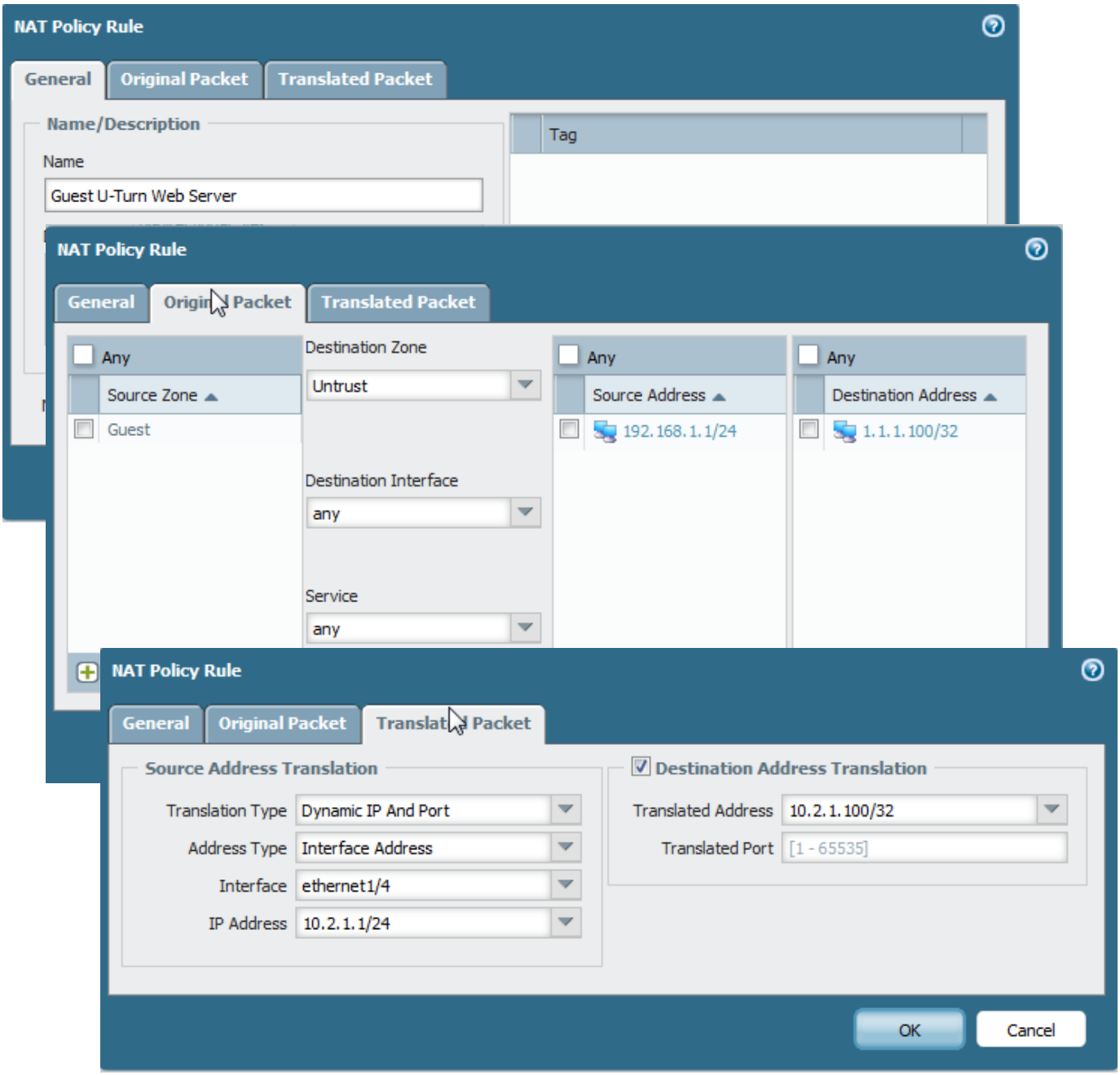
This rule enables the web server to be accessed via the Internet. It translates the destination address of 1.1.1.100 to 10.2.1.100, and translates the source address of the webserver to 1.1.1.100 for outbound traffic from the web server to the Internet.



This rule translates traffic from the Trust zone bound for the public IP address of the web server in the DMZ zone. The public IP must be used as the destination IP address, but the DMZ zone will be used as the destination zone. The destination address of 1.1.1.100 is translated to the DMZ address 10.2.1.100, and the source address is translated to the IP address of interface ethernet1/2.



This rule translates traffic from the Guest zone bound for the public IP address of the web server in the DMZ zone. The public IP must be used as the destination IP address, but the DMZ zone will be used as the destination zone. The destination address of 1.1.1.100 is translated to the DMZ address 10.2.1.100, and the source address is translated to the IP address of interface ethernet1/3.



Security Polices-

	Source		Destination						
Name	Zone	Address	Zone	Address	Application	Service	Action	Pro...	Optio...
Untrust--Trust Webserver	Untrust	any	DMZ	1.1.1.100/32	ssl web-browsing	application-default		none	
Trust--DMZ U-Turn	Trust	10.1.1.0/24	DMZ	1.1.1.100/32	ssl web-browsing	application-default		none	
Guest--DMZ U-Turn	Guest	192.168.1.0/24	DMZ	1.1.1.100/32	ssl web-browsing	application-default		none	
Outbound	DMZ Guest Trust	any	Untrust	any	ssl web-browsing	application-default		none	
DMZ--DMZ	DMZ	any	DMZ	any	any	any		none	
Trust--Trust	Trust	any	Trust	any	any	any		none	
Guest--Guest	Guest	any	Guest	any	any	any		none	
ANY--ANY	any	any	any	any	any	any		none	

Traffic from the Internet (Untrust) to the Web Server-
Source Zone: Untrust
Source Address: ANY
Desination Zone: DMZ
Destination Address: 1.1.1.100/32

Traffic from the internal network (Trust) to the Web Server-
Source Zone: Trust
Source Address: 10.1.1.0/24
Desination Zone: DMZ
Destination Address: 1.1.1.100/32

Traffic from the guest network (Guest) to the Web Server-
Source Zone: Guest
Source Address: 192.168.1.0/24
Desination Zone: DMZ
Destination Address: 1.1.1.100/32