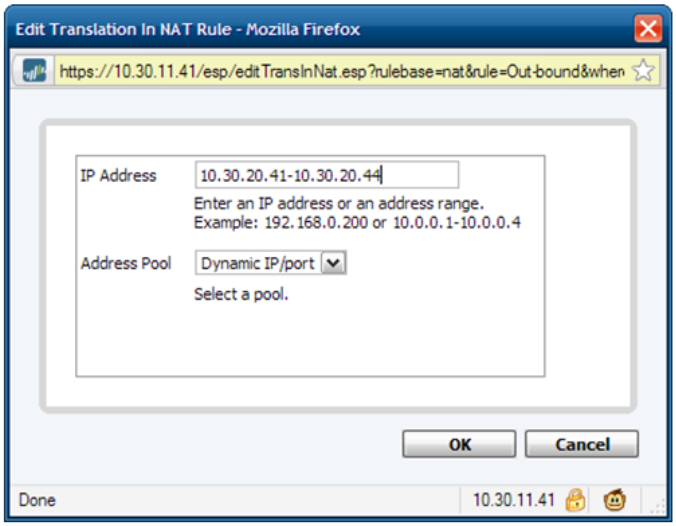
NAT Configuration

PANOS 2.1 and above:

(click on images to enlarge)

Source NAT Pools

- Used when more then one public address is available.
- Needed to support more then 64K out-bound sessions



By specifying multiple IP addresses in the IP Address field a pool is created.

Dynamic IP/Pool:Each connection has both its source IP and Port translated to the next available high port on the next available IP in the pool. The first 64K sessions will be on the first IP and then later addresses will be used, each providing another 64K ports. There is no guarantee that a client will use the same IP in the pool from one session to the next.

Dynamic IP:Each client is assigned the next available IP in the pool. The source port is not translated. The client will use the same IP until there are no more sessions from the client. Then the IP will be returned to the pool for the next client to use. The client is not guaranteed that they will get the same IP address each time. If there are more clients requesting sessions then there are IP addresses in the pool the overflow will not be able to connect until a pool IP is freed up.

Static IP:This is a static one to one mapping of IP addresses in the sourceaddress of the policy to the addresses in the pool. The third address in the source range will be mapped to the third address in the pool every time. Each client is guaranteed the same IP address for each connection. No port address translation is performed. For this to work correctly the address range in the source of the policy should be the same size as the NAT pool. For example the whole 192.168.1.0 range could be mapped to the 10.1.1.0 range, with 192.168.1.10 mapping to 10.1.1.10 and so forth.

This common design is required when the site has a single public IP addressfor a number of services that are provided by different systems internally. This is also referred to as port forwarding or Virtual IP’s (VIP’s). Note that in this scenario the internal web server is running on port 8080 rather then on the traditional port 80.

We use 3 NATrules to forward the correct ports to the three internal servers. Note that all 3 rules have the source and destination zones of “Intranet” as well as having the same destination IP addresses. Additional service objects for ports 25, 110 and 143 are required. Finally we will need to configure the destination translation for the web traffic to be translated to port 8080. The following CLI commands will create these three rules, assuming the service objects and the address object are created.

edit rulebase nat

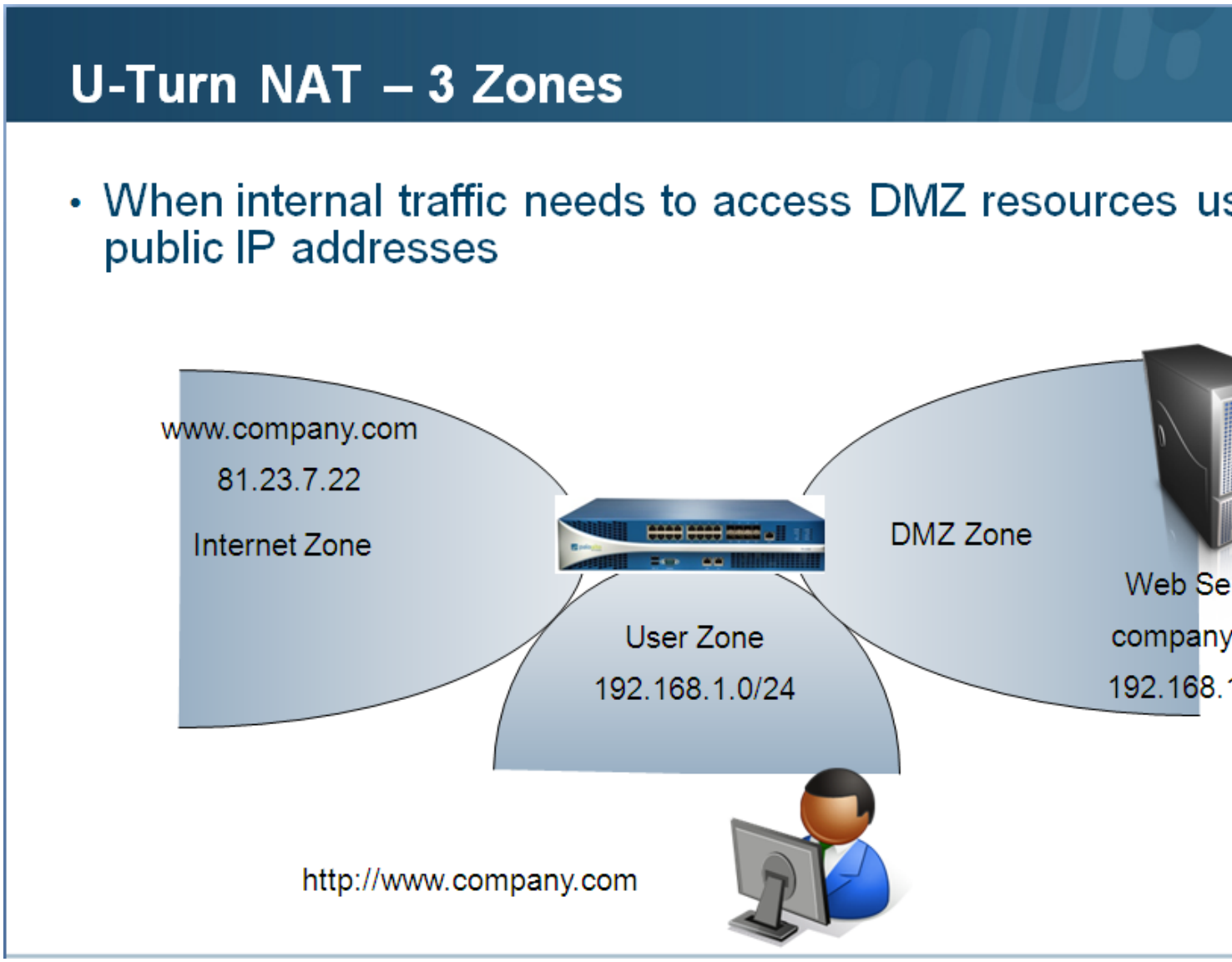
[edit rulebase nat]

set rules "SMTP Relay" from Internet to Internet source any destination Pub_IP-81.23.7.22 service TCP-25 destination-translation translated-address 192.168.10.10

set rules "Web Server" from Internet to Internet source any destination Pub_IP-81.23.7.22 service service-http destination-translation translated-address 192.168.10.20 translated-port 8080

set rules "POP and IMAP" from Internet to Internet source any destination Pub_IP-81.23.7.22 service Mailbox-Access destination-translation translated-address 192.168.10.30

A single security policy will allow the proper access. Remember that allrules use the IP addressing and port information of the original packet. Since none of the initial traffic was using non-standard ports the service of “application-default” is sufficient.



A common designthat can be complex to configure is U-Turn NAT. In the above illustration the company web site for company.com is resolved through public DNS to the IP address 81.23.7.22. The server hosting the actual web site is on the DMZ segment of the firewall at 192.168.10.20. Users in the corporate office on the 192.168.1.0/24 segment need to access the company web page. Their DNS will resolve to the public IP in the Internet zone. The basic destination NAT rules that provide internet users access to the web server will not work for internal users browsing to the public IP.

Keep in mind that all policy rules use the address information of the original packet. In this case the original packet enters the firewall from the User zone and based on routing would

be forwarded to the Internet zone. We need to specify different NATbehavior for this packet then for other user initiated, internet bound traffic. The corresponding security packer has the updated Zones but uses the same address object.

An iteration of the previous designis common in smaller networks. The company web site for company.com is still resolved through public DNS to the IP address 81.23.7.22. However the server hosting the actual web site is on the same segment of the firewall as the users. Users still need to be able to access the server using the public IP address. Their DNS will resolve to the public IP in the Internet zone. The basic destination NAT rules that provide internet users access to the web server will not work for internal users browsing to the public IP.

In this case the original packet still enters the firewall from the User zone and still would be forwarded to the Internet zone. Thedestination NAT will redirect the actual traffic back into the User segment. If we just left the rule the same as in the first example and translated only the destination address, the server would see the request coming from the user IP address and reply directly to the user. This reply would be coming from a different IP address then the request was sent to 9192.168.10.20 rather then 81.23.7.22). To address this issue we need to enable source translation as well on the traffic so that it is returned to the firewall where it can be translated correctly. No security policy is required by default as the traffic is not crossing zone boundaries. Intra-zone traffic is allowed by default.

Authored by the Palo Alto Networks Training.