kenet
Kenya Education Network

ZONE BASED FIREWALLS

BY MICHELLE OPIYO

INTRODUCTION TO FIREWALLS

- Traditionally, a firewall is defined as any device (or software) used to filter or control the flow of traffic. Firewalls are typically implemented on the network perimeter, and function by defining trusted and untrusted zones
- They allow traffic flow from trusted to untrusted zones without specific configurations.

- A firewall isn't limited to only two zones but can also contain multiple less trusted zones (DMZ).
- To control the level of trust in a security zone, each firewall interface is assigned a security level, which is often represented as a numerical value or even color.

FIREWALL SERVICES

- Packet Filtering
- Stateful Packet Inspection
- Proxying
- Network Address Translation (NAT)

PACKET FILTERING

- Packets can be filtered (permitted or denied) based on;

Source Address

Destination Address

Protocol type (IP,TCP,UDP,ICMP etc)

Source Port

Destination Port etc.

- Packet filtering is implemented as a **rule-list**
- The order of the rule-list is a critical consideration. The rule-list is always parsed from top-to-bottom. Thus, more specific rules should always be placed near the top of the rule-list, otherwise they may be negated by a previous, more encompassing rule.
- An implicit deny exists at the bottom of the rule-list.
- Thus, rule-lists that contain only deny statements will prevent all traffic.

STATEFUL PACKET INSPECTION

- Provides services beyond simple packet-filtering, by additionally tracking TCP or UDP sessions between devices
- Stateful inspection can track connections that originate from the trusted network. This session information is kept in a state session table,which allows temporary holes to be opened in the firewall for the return traffic, which might otherwise be denied.

- Connections from the untrusted network to the trusted network are also monitored, to prevent Denial of Service (DoS) attacks. If a high number of half-open sessions are detected, the firewall can be configured to drop the session (and even block the source), or send an alert message indicating an attack is occurring.
- A half-open TCP session indicates that the three-way handshake has not yet completed. A half-open UDP session indicates that no return UDP traffic has been detected. A large number of half-opened sessions will chew up resources, while preventing legitimate connections from being established.

PROXY SERVICES

- Proxies essentially serve as middle-men for communication between devices.
- This provides an element of security, by hiding the actual requesting source. All traffic will seem to be originated from the proxy itself.

NAT

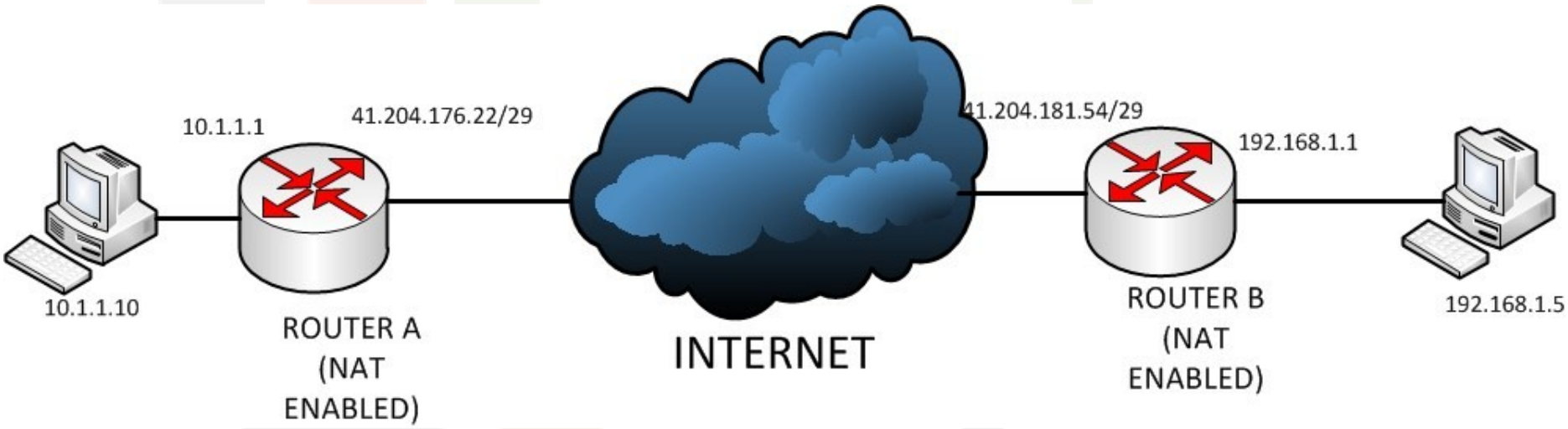
- NAT (Network Address Translation) is used to translate between private addresses and public addresses. (or private to private and public to public)
- Types of NAT;

Static

Dynamic

NAT overload (PAT)

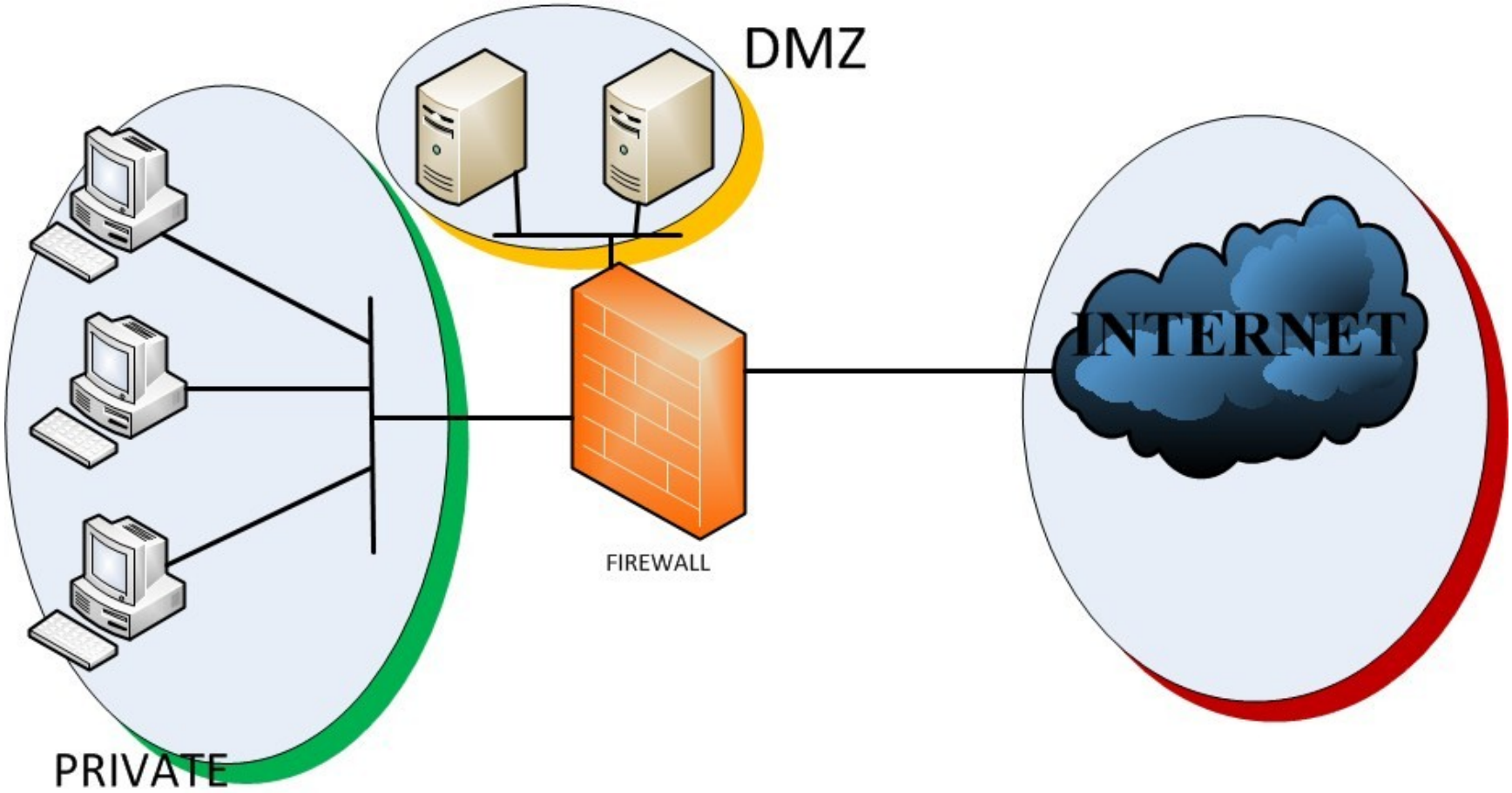
NAT


10.1.1.1
41.204.176.22/29
41.204.181.54/29
192.168.1.1
10.1.1.10
ROUTER A
(NAT
ENABLED)
INTERNET
ROUTER B
(NAT
ENABLED)
192.168.1.5

DMZ

- DMZ is essentially a less trusted zone that sits between the trusted zone (generally the LAN) and the untrusted zone(generally the Internet). Devices that provide services to the untrusted world are generally placed in the DMZ, to provide separation from the trusted network.

FIREWALL DIAGRAM



ZONE BASED FIREWALLS

- Zone based firewalls simply firewall configuration by establishing security borders on your network.

- A **Zone** defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. ZFWs default policy between zones is deny all. If no policy is explicitly configured, all traffic moving between zones is blocked.

- This is a significant departure from stateful inspections model where traffic was implicitly allowed until explicitly blocked with an access control list (ACL).

RULES FOR APPLYING ZONE BASED POLICIES

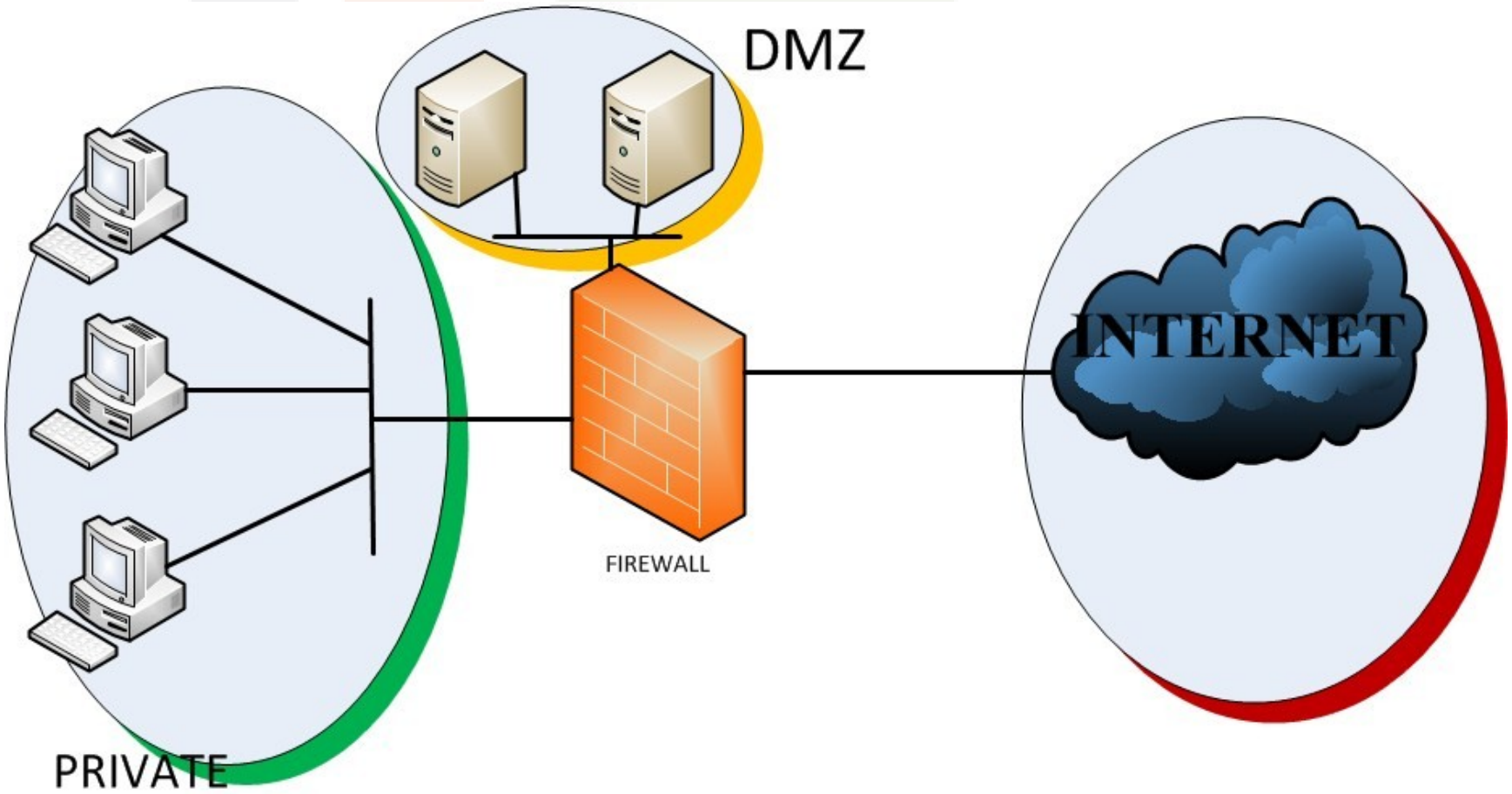
- A zone must be configured before interfaces can be assigned to the zone.
- An interface can be assigned to only one security zone.
- All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

- Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.
- In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.
- The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

- Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones
- If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy)between that zone and any other zone to which traffic flow is desired.

DESIGNING ZONE BASED POLICY NETWORK SECURITY

- Consider an access router with three interfaces:
  - One interface connected to the public Internet
  - One interface connected to a private LAN that must not be accessible from the public Internet
  - One interface connected to an Internet service demilitarized zone (DMZ), where a Web server, Domain Name System (DNS) server, and e−mail server must be accessible to the public Internet


DMZ
INTERNET
FIREWALL
PRIVATE

CONFIGURING A ZFW

1. Define Zones
2. Define Zone-Pairs
3. Define class−maps that describe traffic that must have policy applied as it crosses a zone−pair.
4. Define policy−maps to apply action to your class−maps traffic.
5. Apply policy−maps to zone−pairs.
6. Assign interfaces to zones.

CONFIGURING CLASS-MAPS

- Class−maps define the traffic that the firewall selects for policy application.
- The criteria is specified using the **match** command in a class map eg.

  ACLs

  Protocols (later 4) such as TCP, UDP, ICMP

  A nested class-map

COMBINING MATCH CRITERIA

- **Match any** versus **Match-all** options determine how to apply the match criteria eg,

```
class-map type inspect match-any
  training
match protocol http
match protocol tcp
```

USING ACLs AS MATCH CRITERIA

Class−maps can apply an ACL as one of the match criteria for policy application. If a class−maps only match criterion is an ACL and the class−map is associated with a policy−map applying the inspect action, the router applies basic TCP or UDP inspection for all traffic allowed by the ACL, except that which ZFW provides application−aware inspection.

SAMPLE CONFIGURATION

```
class-map type inspect match-all all-private
match access-group 101
!
policy-map type inspect priv-pub-pmap
class type inspect all-private
inspect
class class-default
!
zone security private
zone security public
zone-pair security priv-pub source private
  destination public
service-policy type inspect priv-pub-pmap
```

```
interface FastEthernet4
ip address 172.16.108.44 255.255.255.0
zone-member security public
!
interface Vlan1
ip address 192.168.108.1 255.255.255.0
zone-member security private
!
access-list 101 permit ip
  192.168.108.0 0.0.0.255 any
```

```
stg-871-L#show policy-map type insp zone-pair priv-pub
• Zone-pair: priv-pub
• Service-policy inspect : priv-pub-pmap
• Class-map: all-private (match-all)
• Match: access-group 101
• Inspect
• Packet inspection statistics [process switch:fast switch]
• tcp packets: [413:51589]
• udp packets: [74:28]
• icmp packets: [0:8]
• ftp packets: [23:0]
• tftp packets: [3:0]
• tftp-data packets: [6:28]
• skinny packets: [238:0]
• Session creations since subsystem startup or last reset 39
• Current session counts (estab/half-open/terminating) [3:0:0]
• Maxever session counts (estab/half-open/terminating) [3:4:1]
• Last session created 00:00:20
• Last statistic reset never
• Last session creation rate 2
• Maxever session creation rate 7
• Last half-open session total 0
• Class-map: class-default (match-any)
• Match: any
• Drop (default action)
• 0 packets, 0 bytes
```

CONFIGURING ZFW POLICY-MAPS

- The policy−map applies firewall policy actions to one or more class−maps to define the service−policy that will be applied to a security zone−pair. When an inspect−type policy−map is created, a default class named class class−default is applied at the end of the class. The class class−defaults default policy action is drop, but can be changed to pass. The log option can be added with the drop action. Inspect cannot be applied on class class−default.

ZONE BASED POLICY FIREWALL ACTIONS

- **Drop**

This is the default action for all traffic, as applied by the "class class−default" that terminates every inspect−type policy−map. Other class−maps within a policy−map can also be configured to drop unwanted traffic. Traffic that is handled by the drop action is "silently" dropped.

- **Pass**

This action allows the router to forward traffic from one zone to another. The pass action does not track the state of connections or sessions within the traffic. Pass only allows the traffic in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. The pass action is useful for protocols such as IPSec ESP, IPSec AH, ISAKMP, and other inherently secure protocols with predictable behavior. However, most application traffic is better handled in the ZFW with the inspect action

- **Inspect**

The inspect action offers state−based traffic control. For example, if traffic from the private zone to the Internet zone in the network is inspected, the router maintains connection or session information for TCP and User Datagram Protocol (UDP) traffic. Therefore, the router permits return traffic sent from Internet−zone hosts in reply to private zone connection requests. Also, inspect can provide application inspection and control for certain service protocols that might carry vulnerable or sensitive application traffic. Audit−trail can be applied with a parameter−map to record connection/session start, stop, duration, the data volume transferred, and source and destination addresses.

- Actions are associated with class−maps in policy−maps:

```
conf t
policy-map type inspect z1-z2-pmap
class type inspect service-cmap
inspect|drop|allow
  [service-parameter-map]
```

- Parameter−maps offer options to modify the connection parameters for a given class−maps inspection policy

CONFIGURING ZFW PARAMETER-MAPS

- Parameter−maps specify inspection behavior for ZFW, for parameters such as DoS protection, TCP connection/UDP session timers, and audit−trail logging settings. Parameter−maps are also applied with Layer 7 class and policy−maps to define application−specific behavior, such as HTTP objects, POP3 and IMAP authentication requirements, and other application−specific information.

```
stg-871-L(config)#parameter-map type inspect
  z1-z2-pmap
stg-871-L(config-profile)#?
```

- parameter-map commands:

Alert Turn on/off alert

audit-trail Turn on/off audit trail

dns-timeout Specify timeout for DNS

Exit Exit from parameter-map

Icmp Config timeout values for icmp

max-incomplete Specify maximum number of incomplete connections before clamping

No Negate or set default values of a command

one-minute Specify one-minute-sample watermarks for clamping

Sessions Maximum number of inspect sessions

Tcp Config timeout values for tcp connections

Udp Config timeout values for udp flows

APPLYING LOGGING FOR ZONE BASED POLICY FIREWALL

- ZFW offers logging options for traffic that is dropped or inspected by default or configured firewall policy actions. Audit−trail logging is available for traffic that the ZFW inspects. Audit−trail is applied by defining audit−trail in a parameter−map and applying the parameter−map with the inspect action in a policy−map

```
conf t
policy-map type inspect z1-z2-pmap
class type inspect service-cmap
inspect|drop|allow
  [parameter-map-name (optional)]
```

QUESTIONS?