DEFENSE IN-DEPTH

PRE-EXAM NOTES

Hussain Ali

NETWORKING

Defense in Depth Pre Exam Notes

This document is designed as a practical, last-minute revision guide. It focuses purely on the configuration tasks, command patterns, and troubleshooting workflows that appear in real lab environments. Every section provides simple explanations and template based commands so the student can quickly recall the required steps without relying on memorizing specific IP addresses or values.

This is not a theoretical textbook. The purpose is to help you understand *what you are configuring*, *why it is required*, and *how to verify it* under exam pressure. All configurations must be customized to match the network topology given in the exam, using the appropriate IP addresses, interfaces, security parameters, and authentication methods.

Use this document as a fast, practical reference to refresh the essential concepts: securing device access, AAA, Zone-Based Firewall, IPS, Layer 2 protections, site-to-site VPN configuration, ASA firewall policies, NAT behaviour, and core troubleshooting commands. Everything included reflects the exact techniques and patterns used in the course labs and real network assessments.

Disclaimer

This document is intended strictly for educational and training purposes.
All configurations, commands, and examples are provided as templates only and must be adapted to your own network environment.
The author assumes no responsibility for any misuse, misconfiguration, or damages resulting from applying these examples in production systems.
Always test changes in a controlled lab environment before deploying them on live networks.

Defense in Depth Pre Exam Notes

Table of Contents

Section 1: Secure Router Access (SSH + Local Login)

Routers must use **SSH only** for remote access.
You need a **domain name**, **RSA keys**, and **VTY lines** set to SSH-only.
Local username is used if AAA server fails.

Command Template:

```
ip domain-name <DOMAIN_NAME>
crypto key generate rsa modulus <KEY_SIZE>
ip ssh version 2

username <USERNAME> secret <PASSWORD>

line vty 0 4
 transport input ssh
```

Section 2: AAA with RADIUS

AAA controls login using an authentication list.
RADIUS server verifies credentials.
If the server is down → router uses local login.

Command Template:

```
aaa new-model

aaa authentication login default group radius local


radius-server host <RADIUS_IP> key <SHARED_KEY>

radius-server host <RADIUS_IP> auth-port <PORT> acct-port <PORT> key <KEY>


line vty 0 4

 login authentication default

 transport input ssh
```

And remember to change the authentication port and authorization port

Section 3: Zone-Based Firewall (ZBF)

ZBF uses **zones** to group interfaces.
A **class-map** matches traffic.
A **policy-map** defines inspect/pass/drop.
A **zone-pair** applies the policy in one direction.

If using "inspect", return flow is automatic.

If using "pass", create a return zone-pair manually.

Command Template:

```
zone security <ZONE_NAME_1>
zone security <ZONE_NAME_2>

interface <INTERFACE>
 zone-member security <ZONE_NAME>

class-map type inspect <CLASS_MAP_NAME>
 match protocol <PROTOCOL_NAME>

policy-map type inspect <POLICY_NAME>
 class <CLASS_MAP_NAME>
  inspect
 class class-default
  drop

zone-pair security <ZONE_PAIR_NAME> source <ZONE_NAME_1> destination <ZONE_NAME_2>
 service-policy type inspect <POLICY_NAME>
```

Section 4: IOS IPS

IPS inspects traffic and blocks malicious signatures.
Enable a signature category and apply it to an interface.

Command Template:

```
ip ips config location <FLASH_PATH>
ip ips signature-definition location <FLASH_PATH>

ip ips signature-category
 category <CATEGORY_NAME>
  activate

interface <INTERFACE>
 ip ips <IPS_NAME> in
```

Remember that the router dose not have the signature package stored in it you have to upload the signature package using the TFTP server

First you have to upload the signature package into the TFTP server

Second use the command “copy tftp://<Router IP>/IOS-S855-CLI.pkg idconf”

Section 5: Layer 2 Security

Protect L2 from attacks like:

- MAC flooding
- DHCP spoofing
- ARP poisoning
- STP manipulation

Port Security

```
interface <INTERFACE>
 switchport mode access
 switchport port-security
 switchport port-security maximum <MAX_MACS>
 switchport port-security violation <MODE>
 switchport port-security mac-address sticky
```

DHCP Snooping

```
ip dhcp snooping
ip dhcp snooping vlan <VLAN_ID>

interface <TRUNK_INTERFACE>
 ip dhcp snooping trust
```

Dynamic ARP Inspection

```
ip arp inspection vlan <VLAN_ID>
```

BPDU Guard

```
interface <ACCESS_INTERFACE>

 spanning-tree bpduguard enable
```

Section 6: Site-to-Site VPN (Router to Router)

VPN needs:

1. Phase 1 policy (ISAKMP)
2. Phase 2 policy (IPsec transform-set)
3. Crypto ACL (interesting traffic)
4. Crypto map attached to the WAN interface

Command Template:

Phase 1

```
crypto isakmp policy <NUMBER>
 encr <ENCRYPTION>
 hash <HASH_TYPE>
 authentication pre-share
 group <DH_GROUP>
 lifetime <SECONDS>

crypto isakmp key <KEY> address <PEER_PUBLIC_IP>
```

Phase 2

```
crypto ipsec transform-set <TRANSFORM_SET_NAME> <ENCRYPTION> <HASH_TYPE>
```

Crypto ACL

```
ip access-list extended <ACL_NAME>
 permit ip <LOCAL_LAN> <WILDCARD> <REMOTE_LAN> <WILDCARD>
```

Crypto Map

```
crypto map <MAP_NAME> <SEQUENCE> ipsec-isakmp
 set peer <PEER_PUBLIC_IP>
 set transform-set <TRANSFORM_SET_NAME>
 match address <ACL_NAME>
```

Apply

```
interface <WAN_INTERFACE>
 crypto map <MAP_NAME>
```

Section 7: ASA Firewall Basics

ASA uses **security levels**, **NAT**, **ACLs**, and **object-groups**.
Inside → higher level
Outside → lower level

DMZ → $0 \geq 100$

Interfaces

```
interface <INTERFACE>

 nameif <NAME>

 security-level <LEVEL>

 ip address <IP> <MASK>
```

Object + NAT

```
object network <INSIDE_OBJECT>

 subnet <INSIDE_SUBNET> <NETMASK>

 nat (inside,outside) dynamic interface
```

ACL for outside to connect to the DMZ

```
access-list <ACL_NAME> extended permit <PROTOCOL> <SOURCE> <DESTINATION>

access-group <ACL_NAME> in interface <INTERFACE>
```

Show Commands

```
show ip interface brief

show running-config

show zone-pair security

show policy-map type inspect

show ip ips all

show ip dhcp snooping binding

show crypto isakmp sa

show crypto ipsec sa

show crypto map

show access-list

show nat
```

Common Exam Breaks

SSH not working

- No RSA key
- No domain name
- Wrong login method

AAA failing

- Wrong shared key
- Wrong port numbers
- AAA method misapplied

ZBF dropping traffic

- Interface not added to a zone
- Class-map not matching
- Using “pass” without return zone-pair

VPN Phase 1 failing

- Wrong peer IP
- Wrong pre-share key
- NAT or ACL interfering

VPN Phase 2 failing

- Crypto ACL mismatch
- NAT NOT exempted
- Wrong transform-set

DHCP snooping failing

- Forgot trust on trunk

ASA blocking traffic

- NAT before ACL
- Wrong ACL direction
- Security levels misused