ASA - FW functionality
Technology between trusted dom and public
packet-filtering - src/dst IP/MAC/Port
application proxy - intermediary agent
stateful inspection - state table, DPI,
NAT, PAT - static, dynamic, 1-1, N-N
zones - sec_level, inside.outside.dmz
traffic permitted from higher to lower

ASA - routing
static routing
easy conf, interface/zone + net + gw + metric
`route INT NET MASK gateway metric`
possible IP SLA tracking
RIP
router rip, version 1|2, passive-interface
no-summary, default-inf originate
authentication
`rip authen mode md5`
`rip authen key KEY key_id X`
distribute-list w/ ACL, std redistribution
OSPF
router ospf, net area, virtual-link,
authentication
redistribution, stub and NSSA area
EIGRP
router ei, network, no-auto, distr-list w/ ACL
authentication md5, split-horiz, redistribution
default-information
IP Multicast
IGMP proxy, IGMP Stub mode
MCast must be enabled, static IGMP group
PIM is enabled by def if mcast is enabled

ASA - FW modes
Context
single-context → std function, one instance
dyn routing, QoS, Mcast
multi-context → like Multi-VRF, Act-Act
no VPN termination
admin context
L2/L3
routed FW → Layer 3, routing, VPN
no non-IP traffic,
transparent FW → L2, switching, no VPN
only two interfaces, no QoS, no MCast

NAT
Network Address Translation
Addr → Addr, 1-1, N-1, N-N
static → bidir NAT, manually configured
dynamic → PAT, 1-N
NAT control + security level
policy-based NAT → NAT+ACL
Identity NAT, NAT Exemption (exclusion)
NAT order
1. NAT exemption
2. Static NAT
3. Static PAT
4. Policy NAT/PAT
5. Identity NAT
6. Dynamic NAT
7. Dynamic PAT

diff between pre 8.4 and post 8.4

Objects and ACLs
ACL - IPv4/v6, access-list and access-group
standard ACL, time-based ACL
object-group → prot, net, svc, ICMP-type
can be nested
content filtering
ActiveX, Java, URL filter
show commands → ACL, asp drop, counters

Modular Policy Framework (MPF)
similar to MQC on IOS
class-map, policy-map, service-policy
L7 protocol awareness - application inspect
SMTP, DNS, FTP, HTTP, VoIP, SNMP, ...
reading L7 proto commands (get, put, auth, ...)
Quality of Service
priority (LLQ), policing, shaping
IPP, DSCP, VPN Tunnel Group
per interface, global
ACL, CM, PM, SP
Other MPF functions
TTL dec, TCP Seq andom, TCP Normal

Context aware FW
security context = virtual firewall
system execution space
config location, interface allocation
admin context
net resources, e.g. AAA, NTP, Syslog
user context(s)
packet classifier - MAC add:
manual MAC
autom generate the MAC for IF
changeto command

Identity-based firewall
creates ACL/rules based on AD info
AD Agent installed on Win Server
AD Agent reachable from ASA
5505 supports 1K users, other 65K
256 groups, 8 IPs per user
object group user

ASA Failover
Interface tests
Link up/down
Net Activity - count of 5secs period
ARP - check last 10 ARP items
Broadcast ping
Stateful/Stateless mode
Parameters must match
RAM, interfaces, feature set
Active/Standby
prim/sec configuration
single-mode
Active/Active
multi-context
prim one context, sec other context
Interfaces
Data, Mngmt, Failover, Stateful

Context-based Access Control (CBAC)
std Cisco IOS FW -secure, per-application
Inspection rule, access-list outside ingress
Process
traffic leaving IN->OUT will create the state
traffic coming from OUT is checked:
if ACL permit, then allow
if ACL deny, then check state table
if state exists then allow
if doesn't exist, drop
Audit trails, intercept tuning
Inspection - TCP/UDP only, no IPSec, no reflACL

Zone-based Firewall (ZBFW)
complex FW - zones, zone-members, zone-rules
security zone = group of interfaces
zone-pair = pair of zones there are tight together
security policy = policy per zone-pair
security pol action
drop, pass, inspect
MPQ - class-map, policy-map type inspect
special zone → SELF
fine tuning - parameter-map

Port-to-Application Mapping (PAM)
adjusting/configuring app non-std ports
`ip pot-map PROT port PORT list ACL`

Identity-based Firewall
user-based Firewall (dynamic per-user pol)
authenticating through AAA - ACS/ISE
configuration
1) AAA
2) identity-policy
3) CM/PM type contol
4) int - ip admission auth

CM - match user-group (type inspect only)
not VRF-aware

Cisco IOS IPS
security feature set
SDEE - Security Device Event Exchange
fail-open capability
not possible to create own sigs, dwnlnd
retire/unretire, enable/disable

Device Administration
Authentication, Authorization, Accounting
Radius, TACACS+
Authentication
ecec, login, dot1x, line, local, rad, tac
Authoization
network, exec, system, command, resources
Accounting
start-stop, ldap
802.1X
client, supplicant - end-device
authenticator - switch/WLC
authentication server - ACS/ISE
port-control mode, force mode
host, multiauth, multidomain, open auth
MAB, guest portal, sponsor portal, web access
EAP betw Auth-client, RADIUS betw Auth-Serv

Cisco Identity Services Engine (ISE)
AAA function, posture, profiling
dot1x control, various eap support
guest portals, web edirect, sponsor portals
possible external DB - LDAP, AD
dynamic VLAN assignment, downloadable ACL
Security Group Access/Tag (SGA/SGT)
redundancy, three modules, logs
support for wireless end-points and WLC
RADIUS support only

Cisco Access-Control System (ACS)
RADIUS for net access, TACACS for user AAA
support for AD, LDAP
operations logs, automated reporting, OSCP
user roles, user rights, auth+auth

RADIUS VSA
Vendor Specific Attribute
IETF definition
av-pair → Attribute+Value pair
call-check, device tracking

Cisco AnyConnect Mobility Client
OS-based client for VPN, dot1x control
wired/wireless access control
tunneling functions
Secure policy control (enterprise level)
Cisco VPN client - no longer exists
Cisco Secure Desktop - no longer exists
Cisco NAC agent - read-only OS tool for gather
provides local posture assessment
various checks - antivir, updates, sys checks
recommend - install updates, AV, upgrade etc

Cisco Secure Access Gateways
IOS/ASA solution
can terminate various types of VPN conns
IPSEC, SSL VPN - see VPN types (sect 6)

Cisco Virtual Security Gateway
- part of the Cisco Nexus 1000v
- provides multitenant granular net access
- L2/L3 mode, high performane - distrib switch
- High Availability, Cloud Secuity
- part of the irtual nexus or nexus cloud service

Cisco Cat 6500 ASA service module
- lower costs, extension to existing Cat6500
- same IOS, more efficiency
- 10M connections, 2G IPSec throughput
- 10K VPN users, 10M NAT xlates, 1000 Vlan
- std redundancy options, 2M ACL entries
- ASA OS min 8.5 and later

ScanSafe Security
- now Cisco Cloud Web Security (CWS)
- cloud-based web-proxy
- instant updates/patches/signatures
- high efficiency for zero-day attacks
- real-time analysis online
- reduces TCO, cloud-based
- web-filter, web-reputation
- AVC - App Visibility Control
- Deployment options
  - NGFW, ISR G2/4000, WSA, anyconnect
- Subscription
  - seat-based, bandwidth-based
- Configuration
  - web-proxy → tower
  - company key

```
parameter-map type content-scan
server scansafe prim IP port http(s)
server scansafe sec IP port http(s)
```

  - interface + cws out

Cisco ESA/WSA
- Email/Web Security Appliance
- easy-to-install, vmware img
- real-time protection
- ESA
  - C170, C380, C680
  - Data Loss Protection
  - detect spam, phishing, track user's click
  - filter, forward, alert
- WSA
  - S170, S380, S680
  - DLP, web-proxy
  - Advanced Malware Protection (AMP)
  - Application Visibility Control (AVC)
  - web reputation filters