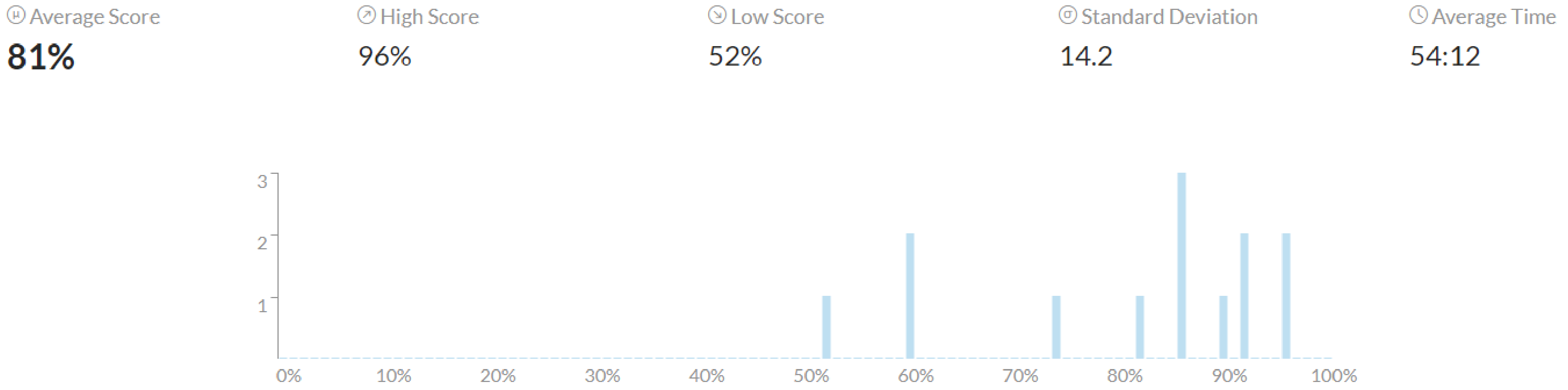
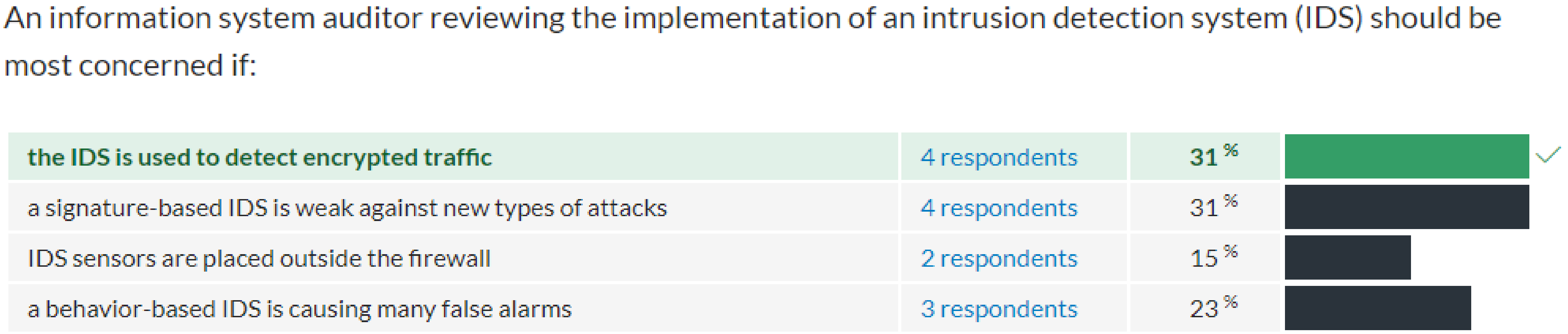
Mid-Term Exam Review

MIS 5214

Summary statistics



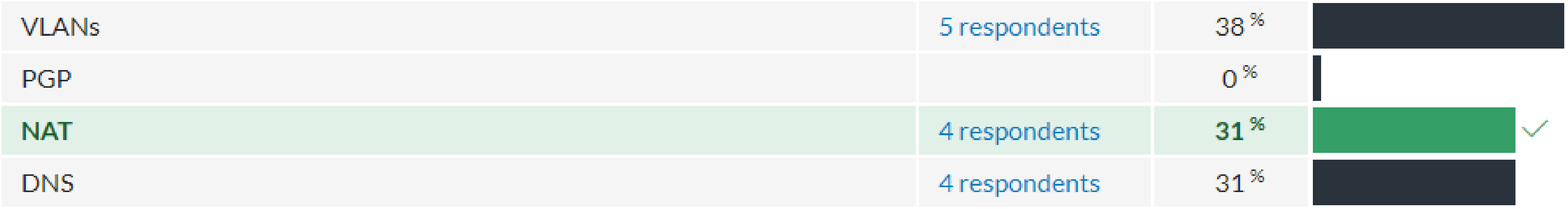
Average Score	High Score	Low Score	Standard Deviation	Average Time
81%	96%	52%	14.2	54:12



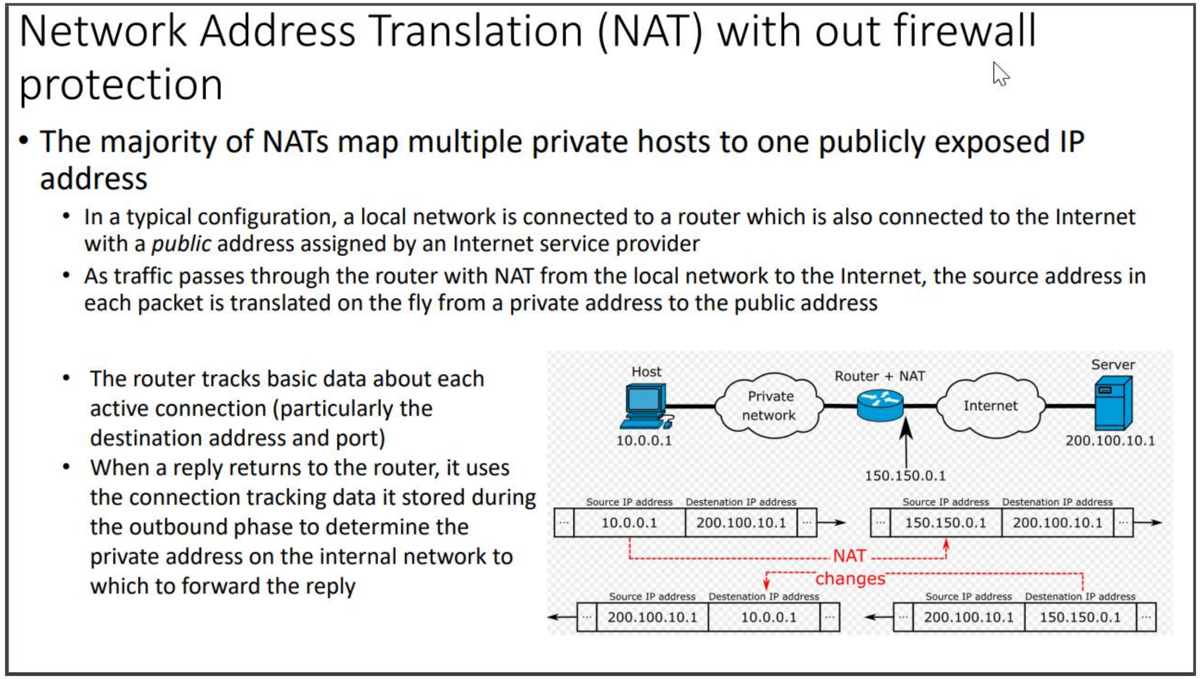
An information system auditor reviewing the implementation of an intrusion detection system (IDS) should be most concerned if:

the IDS is used to detect encrypted traffic	4 respondents	**31 %**	✓
a signature-based IDS is weak against new types of attacks	4 respondents	31 %	
IDS sensors are placed outside the firewall	2 respondents	15 %	
a behavior-based IDS is causing many false alarms	3 respondents	23 %	

While Douglas is monitoring traffic on two ends of a network connection, he sees traffic inbound to a public IP address show up inside the production network bound for an internal host that uses a private internal network reserved address. What technology should Douglas expect is in use at the network border.

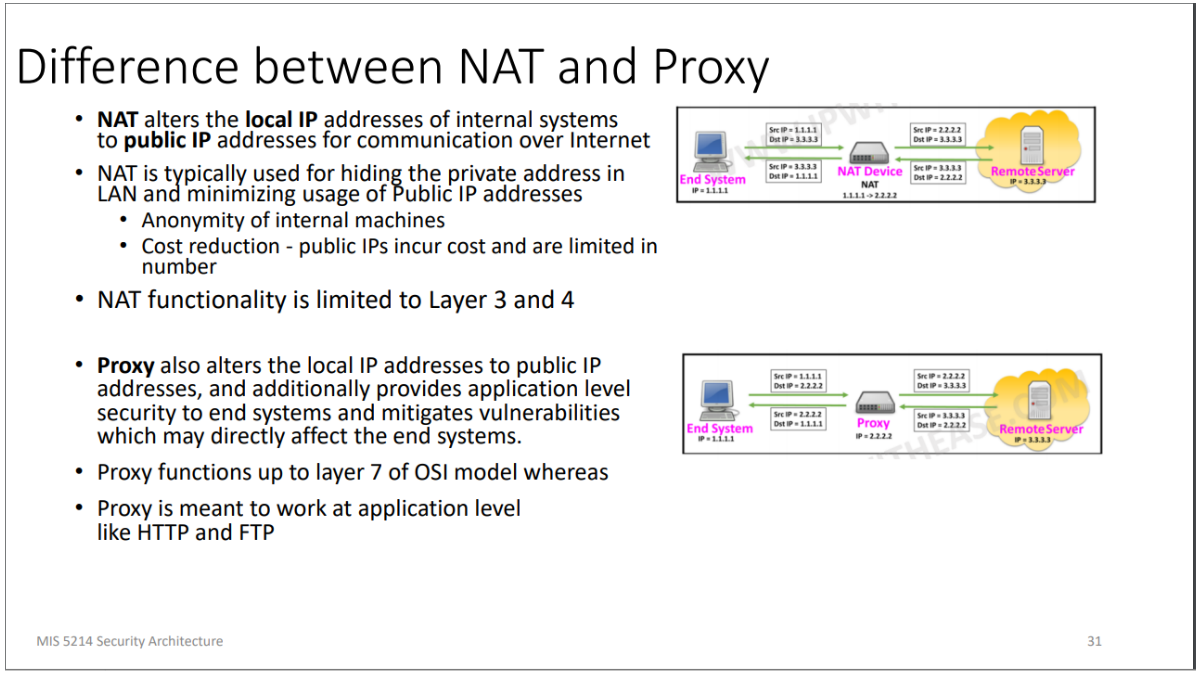


VLANs	5 respondents	38 %	
PGP		0 %	
NAT	4 respondents	31 %	✓
DNS	4 respondents	31 %	



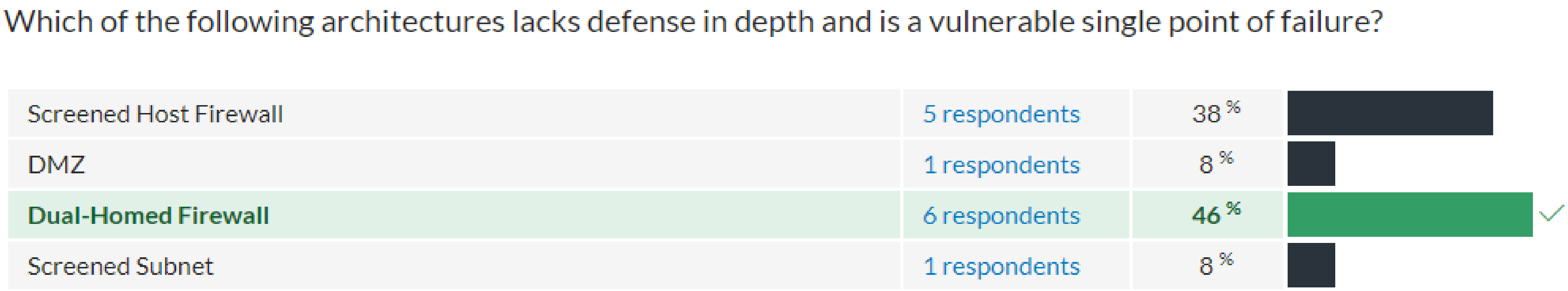
Network Address Translation (NAT) with out firewall protection

- The majority of NATs map multiple private hosts to one publicly exposed IP address
  - In a typical configuration, a local network is connected to a router which is also connected to the Internet with a *public* address assigned by an Internet service provider
  - As traffic passes through the router with NAT from the local network to the Internet, the source address in each packet is translated on the fly from a private address to the public address
  - The router tracks basic data about each active connection (particularly the destination address and port)
  - When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine the private address on the internal network to which to forward the reply



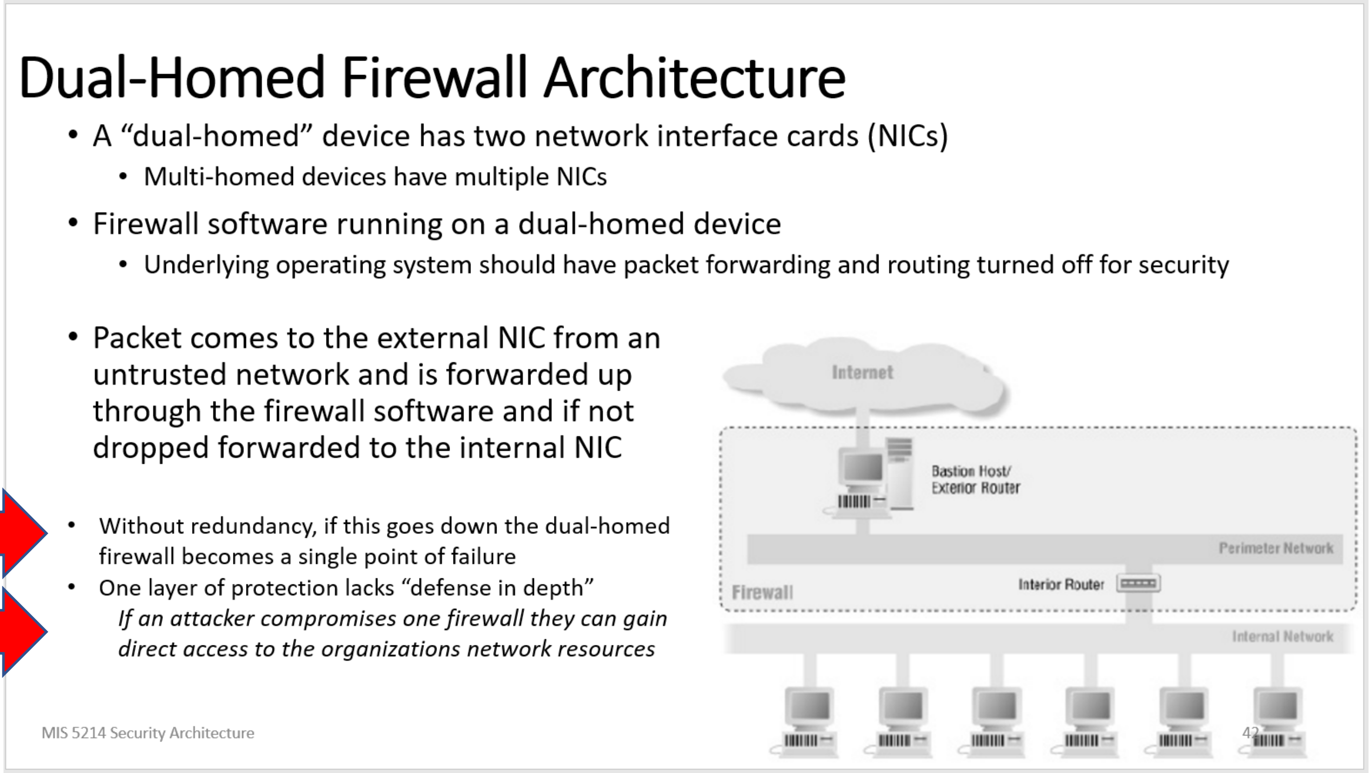
Difference between NAT and Proxy

- **NAT** alters the **local IP** addresses of internal systems to **public IP** addresses for communication over Internet
- NAT is typically used for hiding the private address in LAN and minimizing usage of Public IP addresses
  - Anonymity of internal machines
  - Cost reduction - public IPs incur cost and are limited in number
- NAT functionality is limited to Layer 3 and 4
- **Proxy** also alters the local IP addresses to public IP addresses, and additionally provides application level security to end systems and mitigates vulnerabilities which may directly affect the end systems.
- Proxy functions up to layer 7 of OSI model whereas
- Proxy is meant to work at application level like HTTP and FTP



Which of the following architectures lacks defense in depth and is a vulnerable single point of failure?

Screened Host Firewall	5 respondents	38 %	
DMZ	1 respondents	8 %	
Dual-Homed Firewall	6 respondents	**46 %**	✓
Screened Subnet	1 respondents	8 %	



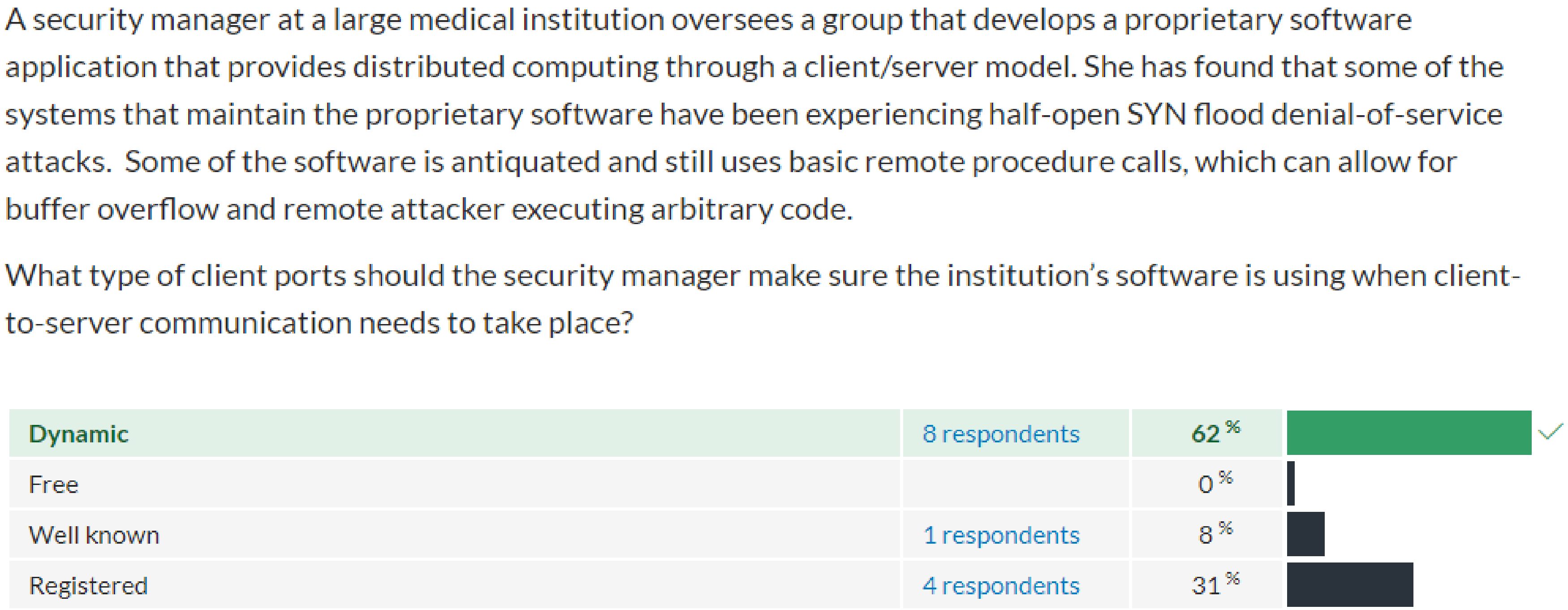
Dual-Homed Firewall Architecture

- A “dual-homed” device has two network interface cards (NICs)
  - Multi-homed devices have multiple NICs
- Firewall software running on a dual-homed device
  - Underlying operating system should have packet forwarding and routing turned off for security
- Packet comes to the external NIC from an untrusted network and is forwarded up through the firewall software and if not dropped forwarded to the internal NIC
- Without redundancy, if this goes down the dual-homed firewall becomes a single point of failure
- One layer of protection lacks “defense in depth”

  If an attacker compromises one firewall they can gain direct access to the organizations network resources

A digital signature contains a message digest to:

Enable message transmission in a digital format	1 respondents	8 %	
Define the encryption algorithm		0 %	
Show if the message has been altered after transmission	6 respondents	**46 %**	✓
Confirm the identity of the originator	6 respondents	46 %	



A security manager at a large medical institution oversees a group that develops a proprietary software application that provides distributed computing through a client/server model. She has found that some of the systems that maintain the proprietary software have been experiencing half-open SYN flood denial-of-service attacks. Some of the software is antiquated and still uses basic remote procedure calls, which can allow for buffer overflow and remote attacker executing arbitrary code.

What type of client ports should the security manager make sure the institution's software is using when client-to-server communication needs to take place?

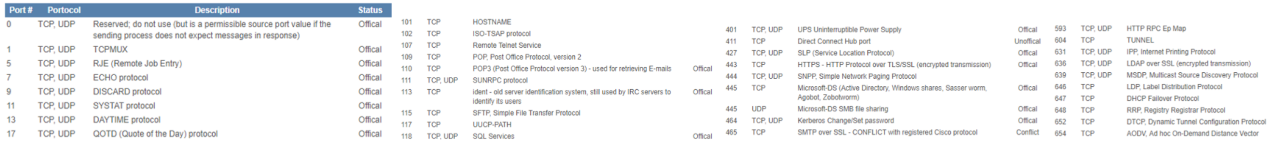
Dynamic	8 respondents	62 %	✓
Free		0 %	
Well known	1 respondents	8 %	
Registered	4 respondents	31 %	

TCP/IP Port numbers

Ports 0 to 1023 are Well-Known Ports

Ports 1024 to 49151 are Registered Ports – Often registered by a software developer to designate a particular port for their application

Ports 49152 to 65535 are Public Ports

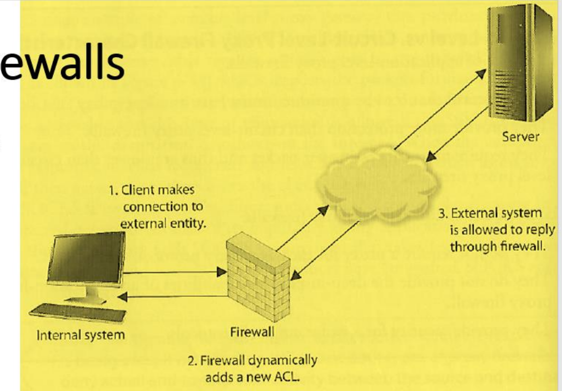


Port #	Portocol	Description	Status
0	TCP, UDP	Reserved; do not use (but is a permissible source port value if the sending process does not expect messages in response)	Offical
1	TCP, UDP	TCPMUX	Offical
5	TCP, UDP	RJE (Remote Job Entry)	Offical
7	TCP, UDP	ECHO protocol	Offical
9	TCP, UDP	DISCARD protocol	Offical
11	TCP, UDP	SYSTAT protocol	Offical
13	TCP, UDP	DAYTIME protocol	Offical
17	TCP, UDP	QOTD (Quote of the Day) protocol	Offical
101	TCP	HOSTNAME	
102	TCP	ISO-TSAP protocol	
107	TCP	Remote Telnet Service	
109	TCP	POP, Post Office Protocol, version 2	
110	TCP	POP3 (Post Office Protocol version 3) - used for retrieving E-mails	Offical
111	TCP, UDP	SUNRPC protocol	
113	TCP	ident - old server identification system, still used by IRC servers to identify its users	Offical
115	TCP	SFTP, Simple File Transfer Protocol	
117	TCP	UUCP-PATH	
118	TCP, UDP	SQL Services	Offical
401	TCP, UDP	UPS Uninterruptible Power Supply	Offical
411	TCP	Direct Connect Hub port	Unoffical
427	TCP, UDP	SLP (Service Location Protocol)	Offical
443	TCP	HTTPS - HTTP Protocol over TLS/SSL (encrypted transmission)	Offical
444	TCP, UDP	SNPP, Simple Network Paging Protocol	
445	TCP	Microsoft-DS (Active Directory, Windows shares, Sasser worm, Agobot, Zobotworm)	Offical
445	UDP	Microsoft-DS SMB file sharing	Offical
464	TCP, UDP	Kerberos Change/Set password	Offical
465	TCP	SMTP over SSL - CONFLICT with registered Cisco protocol	Conflict
593	TCP, UDP	HTTP RPC Ep Map	
604	TCP	TUNNEL	
631	TCP, UDP	IPP, Internet Printing Protocol	
636	TCP, UDP	LDAP over SSL (encrypted transmission)	
639	TCP, UDP	MSDP, Multicast Source Discovery Protocol	
646	TCP	LDP, Label Distribution Protocol	
647	TCP	DHCP Failover Protocol	
648	TCP	RRP, Registry Registrar Protocol	
652	TCP	DTCP, Dynamic Tunnel Configuration Protocol	
654	TCP	AODV, Ad hoc On-Demand Distance Vector	

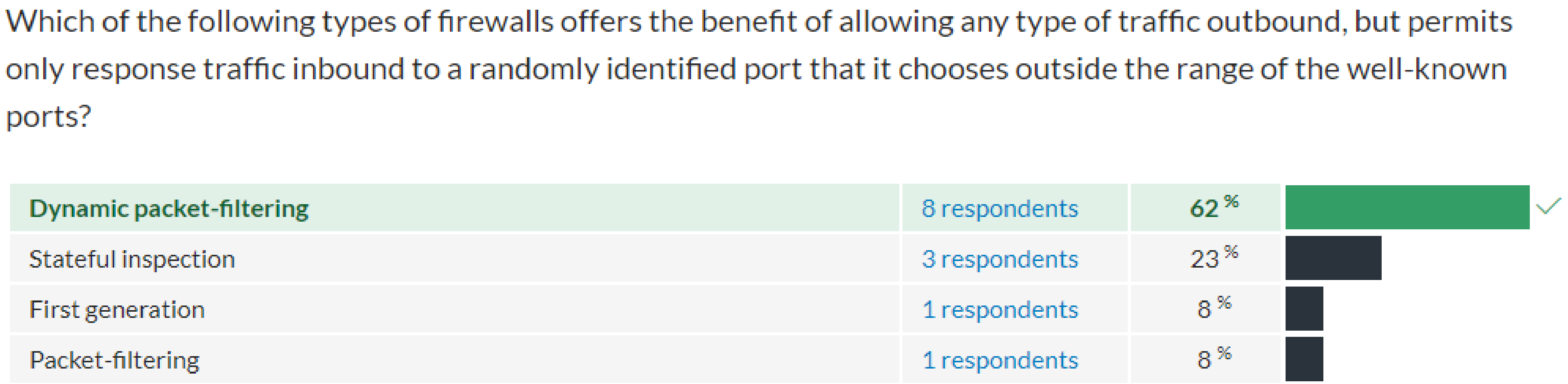
Dynamic Packet-Filtering Firewalls

When an internal system needs to communicate with a computer outside its trusted network it needs to choose an identify its source port so the receiving system knows how/where to reply

- Ports up to 1023 are reserved for specific server-side services and are known as "well-known ports"
- Sending system must choose a randomly identified port higher than 1023 to use to setup a connection with another computer

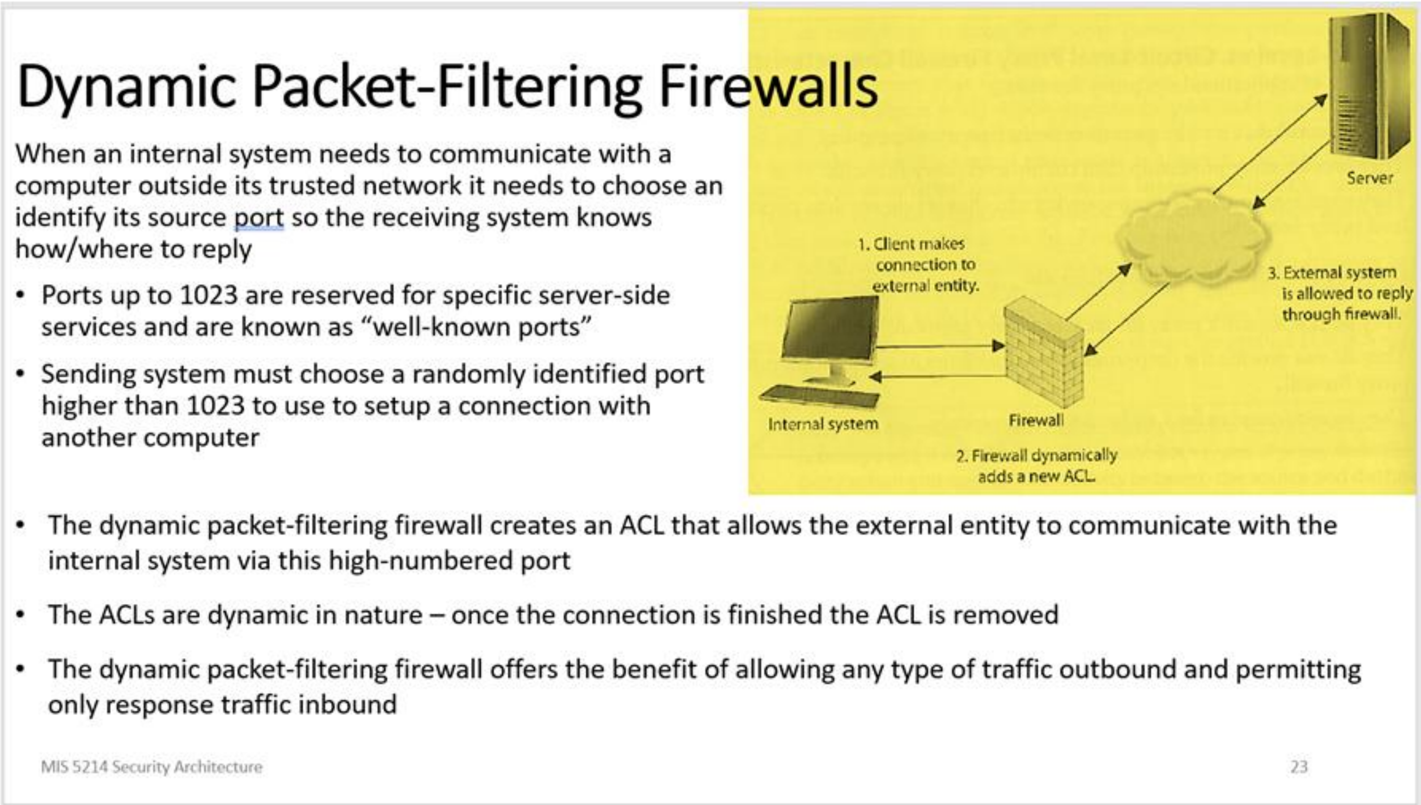

Server
1. Client makes connection to external entity.
3. External system is allowed to reply through firewall.
Internal system
Firewall
2. Firewall dynamically adds a new ACL.

- The dynamic packet-filtering firewall creates an ACL that allows the external entity to communicate with the internal system via this high-numbered port
- The ACLs are dynamic in nature – once the connection is finished the ACL is removed
- The dynamic packet-filtering firewall offers the benefit of allowing any type of traffic outbound and permitting only response traffic inbound



Which of the following types of firewalls offers the benefit of allowing any type of traffic outbound, but permits only response traffic inbound to a randomly identified port that it chooses outside the range of the well-known ports?

Dynamic packet-filtering	8 respondents	62 %	✓
Stateful inspection	3 respondents	23 %	
First generation	1 respondents	8 %	
Packet-filtering	1 respondents	8 %	



Dynamic Packet-Filtering Firewalls

When an internal system needs to communicate with a computer outside its trusted network it needs to choose an identify its source port so the receiving system knows how/where to reply

- Ports up to 1023 are reserved for specific server-side services and are known as "well-known ports"
- Sending system must choose a randomly identified port higher than 1023 to use to setup a connection with another computer

Server
1. Client makes connection to external entity.
3. External system is allowed to reply through firewall.
Internal system
Firewall
2. Firewall dynamically adds a new ACL.

- The dynamic packet-filtering firewall creates an ACL that allows the external entity to communicate with the internal system via this high-numbered port
- The ACLs are dynamic in nature – once the connection is finished the ACL is removed
- The dynamic packet-filtering firewall offers the benefit of allowing any type of traffic outbound and permitting only response traffic inbound

MIS 5214 Security Architecture 23

In The News

- https://www.infosecurity-magazine.com/news/rsac-the-five-most-dangerous-1/
- https://www.afcea.org/content/military-aims-identity-security-trifecta
- https://cybersecuritynews.com/undersea-internet-cables/
- https://www.infosecurity-magazine.com/news/oktaforum-biometrics-privacy-1-1-1-1/
- https://www.wired.com/story/dangerzone-open-email-attachments-safely/
- https://www.infosecurity-magazine.com/news/tmobile-suffers-another-breach/
- https://www.cnet.com/news/dump-your-passwords-improve-your-security-really/
- https://www.securityweek.com/aussie-watchdog-sues-facebook-over-cambridge-analytica-breach
- https://www.securitymagazine.com/articles/91867-whats-driving-identity-access-management-in-2020
- https://www.infosecurity-magazine.com/news/play-protect-ids-just-a-third-of/
- https://www.scmagazine.com/home/security-news/news-archive/coronavirus/five-reasons-why-covid-19-will-bolster-the-cyber-security-industry/
- https://www.infosecurity-magazine.com/news/carnival-cruise-lines-hacked/