Resolução do exame 13/6/2022 (2h)

13 de setembro

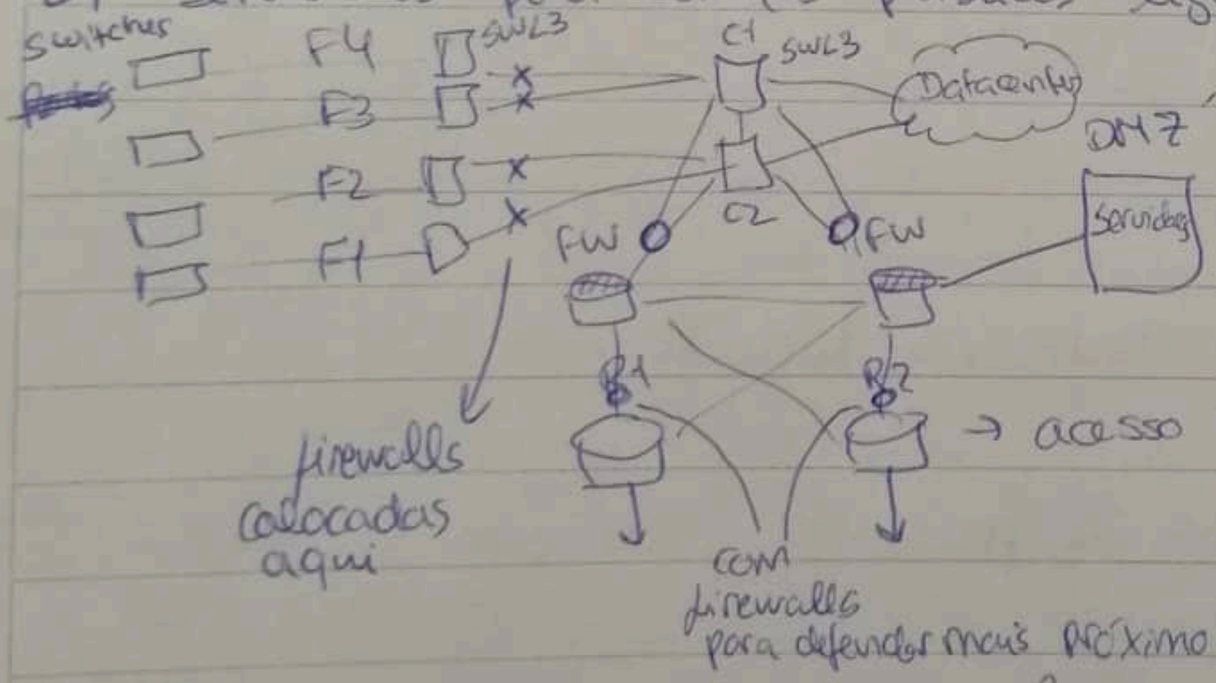
1) vetor de ataque - maneira como atacante pode conseguir atacar a máquina, 1ª fase descoberta (que pessoas tem acesso a serviços...) tentar conhecer as pessoas, tentar obter credenciais de alguém da empresa. (objetivo: tentar enganar alguém da empresa e a partir daí obter mais informação para chegar a alguém mais importante na empresa). Começar por enganar alguém que não tem tantos privilégios, enviar mails com links para introduzir credenciais (fishing). Ou instalar alguma coisa. Ou aceder à máquina fisicamente.

Formas de ataque: mensagens (credenciais / instalar software) / aceder à máquina fisicamente

Filtragem de mensagens, propagação (detetar se máquinas começam a comunicar com outras, que nunca tinham comunicado)

Deteção roubo de dados: monitorização e diferenças de comunicações (regras do género - não pode gerar upload a partir disto) ver como é que os bytes foram transmitidos, coisas estatísticas e de padrões.

2) servidores para serviços públicos ligados à firewall



→ pendurada nas firewalls com memória

o → loadbalancers

precisamos de firewalls statefull (com memória)?

sim, para fazer regras explícitas

se não ~~recebem~~ a regra terá que ser genérica

o que for autorizado num sentido é igual no oposto

defesa de força bruta → colocar mais firewalls sem estarem sincronizadas (cada uma com a sua memória...) para não estarem sincronizadas tráfego deve ser encaminhado pela mesma firewall (com load balancer)

em cima e em baixo da firewall

para controlar tráfego entre as vlans

definir que utilizadores podem aceder ao DMZ
load baloneer garante que manda para a firewall específica para não acontecer firewall ficar sem memória, isto no loadd baloneer de cima e de baixo

3) IPSEC - ESP (confidencialidade)
se for múltiplos pontos tunel multiponto IPSEC-ESP
só tráfego de videoconferencia e sincronismo usam estes IPSEC-ESP
(corte maps)

firewall para estabelecer tunel IPSEC
-regra definir porta da comunicação

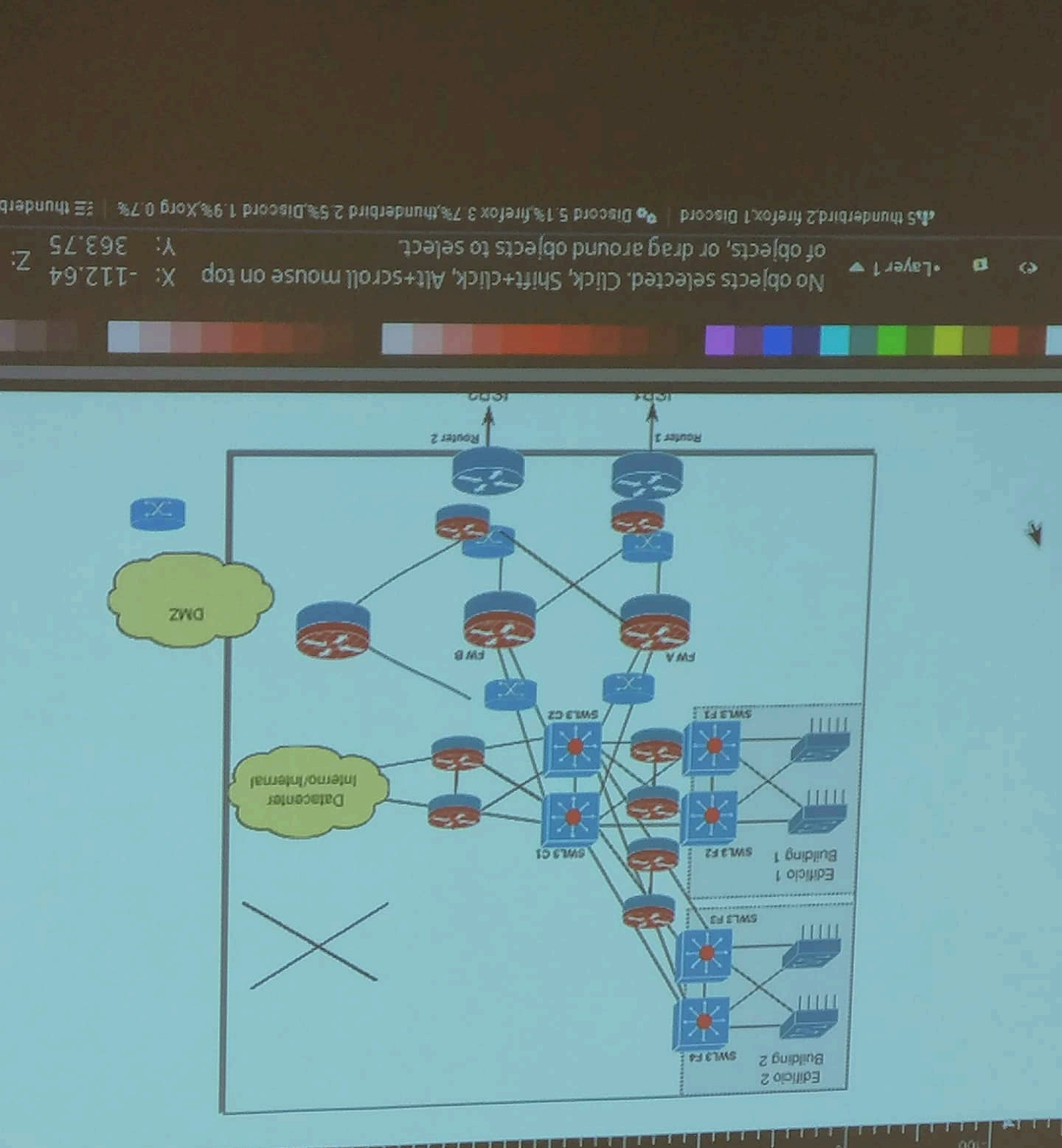
4) 802.1x com RADIUS que pode estar integrado com LDAP
em termos de firewall é preciso ~~[illegible]~~ colocar exceções

5) BotNet - varias máquinas comprometidas que comunicam e formam uma rede

(i) comunicação entre PCs e terminais é pequena
característico de uma BotNet: mais tráfego das VLANs, percaber que a percentagem destas comunicações aumentou
medir matriz tráfego - percentagem de tráfego entre dois pontos (netflow)

SNMP - estatísticas
monitorizar tráfego
(ii) como obter dados, lista HTTPS, dados obtidos na firewall
filtrar quantidades, países
criar evento se alguém comunicar com a máquina, de um país não comum com um IP que nunca comunicou ...
monitorizar eventos

(iii) servidor de email - monitorizar frequência de mails
bots não usam interface web para enviar emails
SMTP
regra: máquina manda mail de hora em hora e começa a mandar de 3 em 3 segundos
se tivermos mail de destino ver se é com domínio da empresa.. ver onde está o servidor


Router 2
Router 1
DMZ
FW B
FW A
SWL3 C2
SWL3 C1
SWL3 F1
SWL3 F2
SWL3 F3
SWL3 F4
Datacenter
Interno/Interenal
Edificio 1
Building 1
Edificio 2
Building 2
No objects selected. Click, Shift+click, Alt+scroll mouse on top of objects, or drag around objects to select
X: -112.64
Y: 363.75
Z:
Layer 1
Help
Path Text Filters Extensions
X: 0.000
Y: 0.000
W: 0.000