**Question on Request for Firewall Configuration Review and Security Assessment**

Answered all the questions below - there are couple of statements that are not really questions – we assume Securium will want to come onsite and check these.

1. can we get firewall config file - access only KIGEN laptop - review only –

Ans - NO, can be reviewed onsite

1. how we do URL filtering ?

Ans - Checkpoint has URL filtering available – no websites exposed so not required

1. is there any duplicate/unnecessary rules exist ?

Ans - There may be

1. is there any inactive rule or that not active form long time ?

Ans - there maybe

1. Inbound/outbound logs ?

Ans - All logged to our ELK system

1. are we following any standards for firewall Cong like NIST , CIS benchmark or ISO271

Ans not that I am aware off

1. do we have any insecure services like HTTP, Telnet and etc on

Ans None

1. do we have secure pass and are we using MFA for accessing firewall admin page?

Ans We have a secure password with unique accounts

1. How NTP synchronies

Ans A central NTP server runs on the network which takes its time from a well know secure NTP server

1. how we handling the Logs ?

Ans Logs are Shipped to a SIEM and central log server

1. firewall OS/Firmware is on latest version ?

Ans Yes

1. do we have any public facing IPs ? how much?

Ans Yes – 4

1. ensure all the rules are well organised for the business requirements

Ans yes

1. do we have any groups for the rules?

Ans Yes, rules are structured

1. ensure that firewall rules are configured on the list privilege for source and destination

Ans yes

1. can we get screenshots for rules which set to denied

Ans yes – you can also see this on site

1. ensure all logging rules are configured at appropriate level specially for inbound/outbound traffic

Ans yes – some really chatty rules may not log to save space(e.g. LAN to LAN DNS)

1. which antivirus we are using , spyware, which tool for vulnerability protection

Ans We have an AV tool running

1. ensure that wild fire profiles are enabled for the zero day threat protection

Ans Firewalls have IDP And IPS software which is up to date

1. ensure that, should not be download malicious e file
2. ensure that net rules are configured correctly that comply with security protocol
3. is there any unnecessary open port are there on internet ?

Ans Not that I am aware off

1. Ensure that our user login are properly monitored
2. ensure that user session are correctly tracked ?

Ans yes

1. ensure that our DMZ are properly designed

Ans yes

1. ensure that our zone protection profiles are applied towards the sensitive zone

Ans yes

1. need to review SSL/TLS decryption policies need to review
2. ensure that firewall are using valid ssl certificated
3. need to review VPN setting including encryption standards and should be strong auth methods
4. Ensure there is limited internal interaction after connecting VPN
5. verify that firewall generating the regular reports for important area like traffic volume, secure incident or VPN usage
6. High availability setup and fail over mechanism are correctly functioning - if applicable
7. ensure that configuration are syncing on primary and secondary device in HA enabled
8. ensure regular automatic backup of firewall configuration are enabled and securely stored
9. in case of backup failure how we restore backup configuration

Ans backup remotely – can be rebuilt and config restored