The National Archives

IT HEALTH CHECK

CLOSING DATE FOR RESPONSES – 5PM, FRIDAY 29TH SEPTEMBER 2017

CLARIFICATION QUESTIONS AND RESPONSES

The National Archives has received a number of clarification questions. These questions and their associated responses can be found below.

Q1: Please would you clarify the approximate number of rules for each firewall?
A1: Approximate rule counts as follows:

Checkpoint – 430
Cisco - 210
Fortinet 1 – 450
Fortinet 2 – 90

Q2: Can we test the 'outside' of the PSN services, from the PSN side of the firewall, as we do not have access to a remote PSN connected link?
A2: Yes, it will be fine to test on-site from the PSN side of the perimeter firewall.

Q3: The document provided lists IP ranges for the external pen test, but not a confirmed figure for live/active IP addresses. To ensure that time is used effectively, can you confirm please the number of live/active external facing IP's that are in scope for this test please?
A3: We would expect around 50 live/active IP addresses on the Internet-facing range.

Q4: In addition to the above, you have also mentioned PSN-facing IP addresses that are in scope for testing. Can you please confirm then number of live/active PSN-facing addresses that are in scope?
A4: We would expect around 20 live/active IP addresses on the PSN-facing range.

Q5: Your document provides full system numbers for servers and workstations, but not laptops or Android mobile devices. Can you confirm full system numbers for these as well, please?
A5: Our figures for workstations include desktops, laptops and tablet PC devices. Android smartphones are remote access devices and will not be encountered during internal testing.

Q6: With regards to the scanning, what percentage scanning sample are you looking for?
A6: We’re looking for the whole estate to be scanned. The figures given in the proposal for servers and workstations represent the expected total number of these in use.

Q7: How many switches are in scope?
A7: We have approximately 70 (logical) switches.

Q8: Do you allow BYOD?
A8: BYO devices are not permitted to access corporate resources. We do operate a public wireless network for personal devices.

Q9: Do you have an MDM solution for remote devices?
A9: Yes, we have an MDM solution for remote devices.

Q10: You've asked for a review of cloud systems -"Verify the security of our network and device configuration allowing use of cloud ITSM, telephony and web/email filtering systems" - could you be more specific please? What cloud systems specifically are in scope for testing, and to what end are they to be tested? Would we test up to the endpoint onsite, or the actual cloud based infrastructure itself? Or would we be specifically testing devices that are designated to access cloud systems? "Verify the security of our network and device configuration" is a little vague.
A10: Configuration items are present on our firewalls and end user devices to allow use of ITSM, telephony, and web/email filtering services which are cloud hosted. The cloud systems themselves are not in scope, only the measures we have taken to allow access to them. It is likely that security verification would take place as part of other tasks, e.g. firewall review and build review: your proposal should highlight where you expect such tasks will fulfil this requirement.

Q11: Section 4.1.2 of the ITT mentions web servers but there are no URL's/Application details provided. Please provide further information for applications considered in scope:

- *URL's*
- *Brief description of service provided*
- *List of user roles that can access the sites*
- *Whether the applications would be tested from an authenticated or unauthenticated perspective*
- *Where they are hosted? (in house or cloud)*

A11: Detailed web applications testing is not in scope here. Web servers and other services present on the Internet- and PSN-facing IP ranges in scope would be generally accessible to Internet and PSN users, hosted in-house, and external testing would be in an unauthenticated manner.

Q12: *Section 4.1.3 of the ITT mentions a build review of each of our operating system builds*

- *Internal test scope mentions virtual servers. The scope in this section doesn't.*
- *Details of virtual servers in scope required.*

A12: Operating system builds are consistent across physical and virtual servers, so this will be a build review of the two different Windows server OS types in use.

Q13: Section 4.1.5 of the ITT mentions security testing of mobile devices, remote access and our use of cloud systems:

- Wireless Network Penetration Test
  - Apart from standard pen test would a review of configuration also be required?
    - Number of rules to review on the Wireless controller?

A13: A review of wireless configuration would be requested. There are no rules there; security rules for wireless connections are on the firewall.

Q14: Section 4.1.5 of the ITT mentions security testing of mobile devices, remote access and our use of cloud systems:

- *Mobile device review*
  - *Any other mobile platforms allowed access on the network?*
    - *How is this managed?*
    - *Are these mobiles corporate provided?*

A14: Other mobile platforms are in operation, but out of scope as they are being decommissioned; this test will look at Android smartphones. Yes, the mobile devices here are managed and provided corporately.

Q15: MDM in place? If so would a review of the MDM configuration also be required? Number of rules/policies to review?

A15: A review of MDM configuration would be requested. Security rules for mobile devices are in place on our firewalls, and policies are by device type – in this case Android smartphones.

Q16: The last point on 4.1.5 also doesn't read right: "Verify the security of our network and device configuration allowing use of cloud ITSM, telephony and web/email filtering systems." The wider scope includes network penetration testing and device configuration reviews in order to verify security. Is this possibly a typo and should read "Review of NETWORK DEVICE". I would then assume that this would be a review of the Wireless Network Controller which I have requested further information on above.
A16: Configuration items are present on our firewalls and end user devices to allow use of ITSM, telephony, and web/email filtering services which are cloud hosted. It is likely that security verification would take place as part of other tasks, e.g. firewall review and build review: your proposal should highlight where you expect such tasks will fulfil this requirement.

Q17: Does the National Archives definitely require the CHECK accreditation or would the CREST accreditation be accepted also?
A17: I can confirm that we definitely require this work to be carried out by a CHECK provider.

Q18: For the internal testing, will a list of internal servers be supplied, or will information on the hosts be based purely on the host discovery exercise?
A18: We would expect internal testing to be based on host discovery, providing the most up-to-date view of devices to test. If there would be some added benefit to providing a list during the test, then we can look into doing this.

Q19: For the external testing, are TNA looking for full manual penetration testing or a vulnerability assessment? If full penetration testing, would it be possible to obtain a list of IP ranges and URLs during the tender process?
A19: Detailed web applications testing is not in scope for the external test. The focus here is on infrastructure and open services visible to the Internet and PSN. This would be without credentials, so we would anticipate a mixture of vulnerability scanning and manual testing activities.

Q20: Can a list of the externally accessible URL's please be provided?
A20: We have approximately 40 root URLs served from our external IP addresses, mostly subdomains under the nationalarchives.gov.uk domain. This includes: www, media, discovery, blog, filestore, elearning. A full list will not be provided at this stage, but this can be given for the test itself if requested.

Q21: For the WiFi, how many networks are involved?
A21: There are two networks: Corporate and Public. Corporate provides secure staff connectivity to our internal network for managed devices, and Public provides Internet access to personal devices.

Q22: Can TNA confirm that the Android mobile device is a single device build?

A22: Yes, we have a single device build for Android.

Q23: What protective marking does the final report require?

A23: The final report would be OFFICIAL-SENSITIVE.