HSCN approach to Split Tunnelling for HSCN access.

HSCN allows remote access services to be provided by CNSP's (Consumer Network Service providers)
Historically, on N3 (TN – Transition Network), Split tunnelling wasn't allowed.
NHS Digital been asked to clarify our position on the use of Split tunnelling for HSCN remote access services in the current COVID-19 situation.

Split-tunnelling - Key risks

NCSC and NHS Digital recognise that networks need to be protected against a number of *key risks*, particularly relevant to Remote access, Inbound Internet connections and Patient Identifiable Data (PID), including:

1. **Exploitation of systems** – The compromise of systems that perform critical functions, affecting the organisation's ability to deliver essential services or resulting in severe loss of customer or user confidence.
2. **Compromise of Information** – The unauthorised access of systems hosting sensitive information directly or allowing an attacker to intercept poorly protected information whilst in transit.
3. **Import and export of Malware** - Implementing appropriate security controls preventing the import and export of malware.
4. **Denial of Service** - Internet-facing networks may be vulnerable to Denial of Service attacks, where access to services are denied to legitimate users or customers.
5. **Bridging of Networks** - The end user device acts as a router between the Internet and HSCN
6. **Local and HSCN internet usage data** - The end user organisation loses sight of the web traffic from that client (from an AUP perspective) - HSCN ANM/SeBo also would not see any of the internet traffic generated by the end user device.
7.

Currently

The Obligations framework and security addendum do not specify if Split tunnelling can or can't be used.
However, NCSC and NIST guidelines recommend against using split tunnels but they don't preclude its use.
NHS Digital understand the need to clarify its stance given the current circumstances.

Covid-19 approach

The use of split tunnels will be allowed for a period of time, however CNSPs must confirm that they are still adhering to all Security obligations as outlined within the HSCN Obligations Framework, including ensuring split tunnelling solution ensures a level of security appropriate to meet CAS(T) and ISO27001 requirements.
Certain specific controls should be implemented to mitigate some of the security concerns that would be manifested by using Split tunnels.
CNSP to ensure it is sending NAS data for all remote access traffic entering HSCN.
NHS Digital will be monitoring the feeds and traffic for suspicious or abnormal traffic.
The client is strongly advised too

- Ensure a firewall is enabled
- Ensure an up-to-date antivirus/anti-malware product is installed
- Ensure if windows 10 the ATP (advanced Threat Protection) is enabled with full logging
- Ensure the operating system is patched with all appropriate security patches.
- Deploy appropriate hard drive encryption where required.

In addition, (but not mandatory) it would be beneficial if the provider's VPN client performed some simple validation of the health and security of the connecting device.

- Does it have a local firewall installed and turned on?
- Does it have Local antivirus and/or Antimalware product installed and running and up to date?
- Is the device running latest operating system level patches (certain OS limitations)

- appropriate hard drive encryption where required.

It is understood that this could take some time to implement and NHS Digital need to ensure we don't hinder existing deployments/sales of Remote access, so would accept a plan to retro fit within a couple of weeks of publication of this guidance.

It is understood that this weakens the overall security of HSCN and reiterate the need for CNSP's to provide IPFix data as per the HSCN obligations framework.

In addition,

CNSPs shall ensure all IP Addresses allocated to the VPN service(s) are registered on the NHS Digital IPAM (HSCN IP Address Management).

CNSPs shall record the following information for each Inbound connection:

- HSCN Consumer Organisation's details
- Customer details
- Destination IP address(s), ports and protocols applications or service details being accessed or provided access to over these VPN services.

CNSPs shall provide NHS Digital's Data Security Centre (DSC) the aforementioned information upon request.

The above is in line with the Obligations on a CNSP who provides Inbound internet and is taken from the HSCN inbound internet connectivity guidelines for CNSPs and consumers.

Rationale

The potential impact that an increased number of remote workers, using HSCN remote access and utilising the Microsoft Teams collaboration and messaging/conferencing solution and other Video conferencing services will have on traffic over HSCN infrastructure and its central services could be quite large depending on several factors around the uptake of that NHSMail Teams service.

In addition, corporate windows 10 devices with ATP enabled would send a large volume of traffic which doesn't need to traverse HSCN and ANM.

To reduce the impact on HSCN central services (Peering Exchange, ANM and Secure Boundary) and to potentially improve the users experience, NHS Digital wish to make an allowance around using Split tunnel VPN's for access into HSCN during the Covid-19 pandemic.

However, the advice on using split tunnelling is only a COVID-19 response and will be reviewed on a monthly basis. This statement is being made having performed some analysis on the solutions deployed already, and a risk assessment defining the risks and mitigations NHS Digital feel are required.

Longer term approach

A longer-term approach to remote access standards will be worked on to ensure an appropriate set of security requirements and standards are specified for Remote access services. The current approach will be reviewed on a monthly basis. Any changes would be directed through the standard HSCN change process and would be directed via the HSCN Compliance group and through Inopsis to the CNSP community for response.

HSCN consumers are also advised to review the following guidance:

- Protecting your organisation from ransomware

Supporting information

- Microsoft Direct Access utilises Split tunnelling
- https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/vpns
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NHS Digital's guidance on inbound HSCN internet connectivity:
- Network security guidance for health and care organisations
- https://docs.microsoft.com/en-us/microsoftteams/prepare-network