18.7. Inverse split tunnel VPN

Objective

18.7.1. Agencies identify and effectively manage the risks and compensating controls involved in utilising inverse split tunnelling as part of remote access virtual private network (VPN) configurations.

Context

Scope

18.7.2. This section covers information relating specifically to configuring secure remote access services (also known as VPN services) for agency devices that facilitate agency information (e.g., documents or emails) being transferred to remote systems.

18.7.3. It is important to recognise that all systems that are able to hold or access agency information need protection from compromise.

18.7.4. Traditional network design approaches have focussed on keeping agency information within a defined perimeter unless it is explicitly released through an approved gateway (such as via an email or file transfer system), even when being accessed remotely.

18.7.5. There are a number of prevalent architecture patterns for delivering remote access services that support this traditional network design approach. Typical patterns include:

a. Always-on VPN services from agency-owned or agency-managed devices.
b. As-needed VPN services from agency-owned or agency-managed devices.
c. Remote desktop, or thin client, services from any devices, including BYOD.
d. Remote, or virtual, applications accessed from any devices, including BYOD.

18.7.6. With an accelerated adoption of cloud delivered services, and agency moves to increase the level of work being performed remotely through online collaboration systems, the government has published advice on the use of inverse split tunnel architectures for remote access VPN services to improve performance.

18.7.7. The architecture advice advocates for the use of inverse split tunnelling, where an explicit list of authorised and trusted internet based services are able to be directly accessed, bypassing agency perimeter controls. Both the architecture advice, and the NZISM, advise against the use of full split tunnelling (i.e., allowing all internet traffic not destined to the agency internal networks to bypass agency security controls).

18.7.8. The use of inverse split tunnel VPN configurations is most likely to be appropriate for agencies that are implementing Zero Trust Architecture approaches to network security.

18.7.9. Inverse split tunnel VPN configurations have related, but different, considerations from designs that only support direct access to agency-managed cloud services from the internet (where devices do not also connect to a remote access VPN service).

18.7.10. It is also important to recognise that directly accessed services represent cross-connectivity between systems and must be carefully controlled in order not to compromise trust zones. The principles of separation and segregation must be applied. These principles are discussed in section 22.1 – Cloud computing, and section 22.2 – Virtualisation.

18.7.11. Cross-connection of systems may also create a gateway, whether or not it meets the technical definition of gateways. It is important to refer to section 19.1 – Gateways, and section 19.2 – Cross domain solutions to understand the implications and relevant controls.

18.7.12. In addition to this section, split tunnelling advice is further described in section 21 – Distributed working.

References

18.7.13. Further references can be found at:

Reference	Title	Publisher	Source
	Guide to optimising network traffic for cloud services	GCDO	Guide to Optimising Network Traffic for Cloud Services | NZ Digital government

Rationale & Controls

Inverse split tunnel in remote access VPN systems

18.7.14.R.01. **Rationale**

Remote access VPN services that utilise any form of split tunnelling provide a mechanism for agency devices to connect directly to third party services, bypassing the traditional perimeter. While this provides efficiencies in network routing and can improve agency worker's device performance, it introduces a broader range of threats and vulnerabilities to be considered.

18.7.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7250]

Agencies MUST undertake a threat and risk assessment on the use of inverse split tunnelling prior to enabling the functionality in remote access VPN systems.

18.7.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7251]

When providing inverse split-tunnelled access to internet based services ("directly accessed services"), the following aspects SHOULD be considered as part of the threat and risk assessment:

- How do directly accessed services authenticate agency device identities prior to granting access to the service?
- How do agency devices securely resolve internet addresses for directly accessed services?
- How are the communications between the devices and directly accessed services secured?
- How does an agency monitor and account for access made to directly accessed services?
- How does an agency protect devices from compromise if they are able to directly access internet based resources, or be directly accessed from the internet?
- How do directly accessed services authenticate the user of the agency device prior to granting access to the service (this is separate to authenticating the agency device itself)?
- How does an agency enforce the use of multi-factor authentication with directly accessed services?
- How does an agency authorise access to directly accessed services, and does this include from devices that are not authorised to connect to agency remote access services (authorisation and authentication are separate activities)?
- How is access to directly accessed cloud services removed when staff no longer require access or leave the agency?