|  |  |  |  |
| --- | --- | --- | --- |
| Project no / reference: | | 1 | |
| Project name: | | Design and development of software tools for the improved protection of networks | |
| Date updated: | | 25 March 2024 | |
| Business address: | | 6 Maud Street UNLEY, SA 5061 | |
| Start date: | July 2021 | Finish date: | June 2023 |

# Background and Technical Objectives

|  |
| --- |
| **What are the objectives of this project? (50 – 1,000 characters)** |
| Design Networks Pty Ltd (“Design Networks”) aims to create a viable approach to improving corporate network security, by monitoring, filtering and blocking outgoing traffic and integrating the network traffic filtering with a Zero-Trust Architecture (ZTA). The combination of network filtering and ZTA will reduce the opportunities for a malicious actor. R&D work is required in developing the software tools to facilitate the use of this approach.  Moving forward our aim is to use the core design of extended DNS data to produce clients on Windows X86, Linux Arm, pfSense (BSD), Router and switch hardware. The clients would actively setup filtering of DNS and IP addresses associated with attempts to access locations that are registered in the DNS as Bad  *During collation of the FY23 Application, Design Networks has been referred to the latest AusIndustry Guidance and sought to only register as Core R&D Activities elements of their platform where:*   * *They are developing a tangible new function that has generated new technical knowledge;* * *The outcome of how to develop this function was not able to be determined in advance based on existing knowledge.*   *Effort during FY23 related to standard development, customisation or maintenance has NOT been registered as a Core or Supporting R&D Activity.* |

# Research and Development Activities

|  |  |  |
| --- | --- | --- |
| Core Activities Description | | |
| Core Activity 1: Design, development and testing of a DNS filtering service | Start date:  Jul 2021 | End date:  Jun 2023 |
| **What was the hypothesis? (50 – 4,000 characters):**  A Domain Name System (DNS) server is a server for translating domain names (e.g. google.com.au) to one or more IP addresses (e.g. 198.0.2.1). DNS servers are part of the core infrastructure of the internet.  The hypothesis is that a DNS server is best placed to apply domain and IP filtering rules and, if successful, these rules could be easily integrated to a corporate network without the need for special and expensive hardware-based solutions. A DNS based filtering service would be easily integrated to support other solutions.  The intent is to develop a custom DNS server that would provide the same functionality as standard servers while implementing domain and IP filtering rules. High risk domains would be blocked so queries for any high-risk domains would return a private IP address (e.g. 127.0.4.11) instead of the actual IPs assigned. Further, for domains that are not blocked, the IPs returned in the answer would be checked and any IPs that were considered a risk would be removed from the answer. Where all IPs for a given domain are considered a risk, the domain would be effectively blocked.  The data in the lists will be categorised by type of risk to enable sites to be selected by users. An example of grouping would be Porn, Gambling, Advertising, and News. These could be selectable while Child Porns, Virus sites, anything that is illegal, etc.  As browsers and other applications rely on DNS servers to perform the domain to IP translation, returning a private IP address to the application would result in the application being unable to connect to the domain. For a browser user, instead of the home page for the domain being displayed, it would appear as the web site was not available. Hence users would be restricted to visiting web sites deemed not to be high risk.  The filtering DNS server would apply the same rules data as implemented by the on-premises server but, as it complied with relevant RFCs and standards, it would have more application and a more flexible implementation process for more corporations. The DNS server could therefore implement the core logic of the on-premises server but remotely and from any client that implemented the ubiquitous DNS protocol.  Specific quantifiable objectives include that the DNS created by Design Networks is to be accurate to > 99.5%, and facilitate > 2,000 peak queries per second with >1,000 concurrent users.  A white list will be added to the function of any client to allow individual users to authorize access to any site which has been marked as a risk.  Additionally group lists for a corporate could be integrated to reduce setup time for new users  Logs from all clients would produce significant intelligence on what are common sites and any potential background tasks that are becoming active  In FY23, work focused on   * Implementing the solution for client software * Improving the scalability and performance of the solution * Adding an authorisation method to effect customer policy * Adding an authentication method to identify customers * Adding a partitioning scheme to allow multiple groups of customers to share the same server with different policy applied * Implementing custom policy and rules to satisfy edge cases and non-compliant Internet DNS * Creating new EDNS tags to extend standards * Logic to provide an unfiltered view as additional data in the response to allow client observation of effectiveness   … / the hypothesis was updated to move beyond the proof of concept to develop a product that would address customer wants and needs in the real world | | |
| **Did you conduct this core activity for a substantial purpose of generating new knowledge?**  Yes.  *(Populated by default - a core activity must be conducted for at least a substantial purpose of generating new knowledge.)* | | |
| **What new knowledge was this core activity intended to produce? (50 – 1,000 characters):**  The intention of this activity is to generate new knowledge in the form of an understanding of:   * How to implement very large domain and IP rulesets using internet standard DNS servers; * How to control and manage access to a filtering DNS server using EDNS fields; * How to apply filtering rules at scale and with no practical performance impact from a user perspective. * How to group different rules together for user to select levels of protection * How to consolidate user logs to provide advance risk assessments of user activity * How to manage multiple client in a single front end of a Managed service provider MSP to control a larger group of users. * How to update the DNS data based on current user activity for both good and bad sites. * How to inform users about activity   Similar solutions exist, including:   * AbuseDB is a simplified version of the database; however, it is only based on a firewall incoming protection model and does not have data on web site specific dangers, rather than incoming SSH, and port scanning; * There are advertising stopping features available for users but not security focused services that are generally available.   Incorporating a set of function from protection, to stopping traffic, and redirecting to a renderer all working together is new and innovative.  Additional new knowledge sought to be generated from experimentation conducted in FY23 includes…   * Identify edge cases and exceptions to rules processing * Confidence in policy compliance for the solution * Comparing our high-performance in-band authorisation solution to external solutions such as VPN * Ideal logical location (ie: network/packet/lookup/database/filesystem) to implement caching and sharding strategies for a scalable high performance solutions * Trial different rulesets from other vendors to measure their effectiveness as an alternative on our platform | | |
| **How did the company determine that the outcome could not be known in advance?**   * There was no applicable information in scientific, technical, or professional literature or patents:   + True * Experts in the field provided advice that there wasn’t a solution that could be applied:   + True * There wasn’t a way to adapt solutions from other companies in, and out of, Australia:   + True | | |
| **Please explain what sources were investigated, what information was found, and why a competent professional could not have known or determined the outcome in advance (i.e. technical unknowns). (50 – 1,000 characters):**  Extensive research was undertaken (see Supporting Activity 1) to supplement the company’s expertise, but Design Networks couldn’t have leveraged existing knowledge. Existing solutions (noted above) have limitations that Design Networks aims to overcome.  Technological unknowns relevant to FY23 include   * Performance under load from multiple customers * Caching outcomes at multiple layers in the solution and interactions between different caches * Operation of the solution in a cloud rather than local environment * Distribution of the application over multiple regions and the effect of latency on performance and user experience of the solution   … and research conducted to seek to identify the existing state of knowledge and resolve these unknowns includes…   * Setting up test environments in disparate locations * Developing testing models and harnesses * Iterating the tests with improvements and changes to code | | |
| **What was the experiment and how did it test the hypothesis? (50 – 4,000 characters):**  Work undertaken in FY23 involved the following:   * Development of… * Test systems and harnesses * Large scale tests and software to analyse and tabulate the results * Negative cases * Identifying historical DNS anomalies * Conducting testing… * Running Tests * Improving and modifying code to respond to test results, particularly compliance * Re-iterating tests   Key variables include:   * Design of the DNS, including:   + Use of bind and/or PowerDNS;   + Design of scripts;   + DNS modifications made by Design Networks; * Size and scale of the rules data; * Deployment environment (e.g. speed of processor, allocated RAM, etc.); * Performance: Accuracy > 99.5%, > 2,000 peak queries per second with >1,000 concurrent users; * Compliance with RFC (request for comment) standards. | | |
| **How did you evaluate or plan to evaluate results from your experiment? (50 – 4,000 characters):**  A test suite was developed in parallel to the filtering DNS server that used the same rules data to perform queries on a filtering DNS server with known, expected results. The actual results were compared with the expected results and discrepancies logged for later investigation.  Unexpected results could be caused by:  Missing/corrupted data in the DNS rules;  An issue in the DNS server rules logic;  An issue in the test suite application of the rules data or logic.  Load performance was tested by simulating many concurrent users issuing queries. The test suite generated many worker threads (> 1,000) with each worker thread performing queries to the DNS server under test as quickly as possible. The results of all the queries from all the threads were stored in a database for later analysis. The performance of the DNs server could be measured as:  Peak queries answered per second;  Min/max/average response time per query;  Distribution of response times.  The company observed the following in FY23:   * What test results did you get? * We were able to achieve performance that was significantly better than a hardware appliance that had been developed alongside the rules database * 2 orders of magnitude greater capacity * Signficant improvement in latency (3ms for lookup vs 600ms) * Operation on significantly reduced hardware requirements (80Gb memory) vs an alternate solution implemented by another party on AWS Elasticache (2Tb memory) with the same ruleset * What technical issues, failures or challenges occurred? * The stable releases of PowerDNS did not scale our solution well * A high-performance JIT-compiling library for the embedded scripting only supported 32-bit maths, whereas our high-speed auth function needed 64-bit operations for secure operation * We identified some “no win” scenarios where real-world servers could be part of a cluster where some servers were identified as malicious but others were not, and direction to individual servers was out of our control or hidden behind an alias mechanism * What modifications did you make in response to the technical challenges? * We developed our own math library to support a necessary 64-bit function (modulus/division) on 32-bit architecture * We developed logic to handle scenarios where the answer could not be known ahead of time, such as where nested CNAME lookups might direct DNS to a blacklisted server, or an NS record was itself handled by a potentially compromised server * We altered our testing methodology to accept a statistically insignificant number of false positives as compliant with the rules * What was the result of these tests / modifications – i.e. was the design successful or will further changes be required? * The design was successful – data was transmitted by the server, received by the client, analysed locally then filters applied to on going traffic.. Tested to show ip address was not allowed in negative cases.. | | |
| **Describe the conclusions reached from your experiments in the selected income period. (50 – 4,000 characters):**  As of 30 June 2023, the hypothesis was proven …  Ultimately as a result of experimentation and iteration, we were able to produce a new solution which was faster, cheaper and more compliant than alternate solutions on the same ruleset  In future financial years…  **Will expand capabilities of server to include more details, add client base and centralise A MANAGEMENT SYSTEM TO CONTROL ALL CLIENTS AND SEE ALL LOGGED DATA** | | |

|  |  |  |
| --- | --- | --- |
| Core Activities Description | | |
| Core Activity 2: Design, development and testing of a Zero-Trust architecture with DNS and IP filtering of external connections | Start date:  Jul 2021 | End date:  Jun 2023 |
| **What was the hypothesis? (50 – 4,000 characters):**  Zero-Trust is a high-level strategy that assumes that individuals, devices, and services that are attempting to access company resources, even those inside the network, cannot automatically be trusted. To enhance security these users are verified every time they request access, even if they were authenticated earlier.  It is hypothesized that while Zero-Trust environments provide a high level of security and confidence between trusted endpoints, there is a need to enable access to resources outside of the Zero-Trust architecture (ZTA) without compromising security. Currently, access to resources outside of the ZTA is either allowed and unmanaged, or not allowed at all, which can be overly restrictive and encourage users to bypass security mechanisms. To address this issue, it is suggested that a system be developed that allows for the secure and controlled sharing of resources outside of the ZTA. This could involve implementing a policy-based approach that determines which resources can be accessed by which endpoints, based on factors such as the identity of the endpoint, the sensitivity of the resource, and the context of the request. By implementing such a system, organizations can maintain the high level of security and confidence provided by Zero-Trust environments, while also enabling more flexible access to resources outside of the network. Ultimately, this could lead to more efficient and effective use of resources, as well as enhanced security and compliance.  The specific objective is that Design Networks can integrate the DNS filtering service to a ZTA, to better protect users when they access domains and IPs on the public internet, outside the protection of the zero network, while maintaining DNS performance (i.e. accuracy, scalability and speed as in Core Activity 1).  In FY23, work focused on… / the hypothesis was updated to…  Focus on the client controls for filtering and access to the public network. Automate updates of filtering, add whitelists for groups and local users to over ride negative cases… Add grouping in filtering for possible choice by the user such as porn, gambling, sexist, extreme political, etc | | |
| **Did you conduct this core activity for a substantial purpose of generating new knowledge?**  Yes.  *(Populated by default - a core activity must be conducted for at least a substantial purpose of generating new knowledge.)* | | |
| **What new knowledge was this core activity intended to produce? (50 – 1,000 characters):**  New knowledge was generated in the form of an understanding that it was possible to, and how to, add DNS and IP filtering services to ZTA without impacting performance or usability.  Existing Zero-Trust solutions protect users only while accessing services within the ZTA; the network could still be compromised by a malicious actor through users accessing untrusted domains and IPs.  Additional new knowledge sought to be generated from experimentation conducted in FY23 includes…  Flexibity of DNS system, addition variable to be accessed, how the external dns system could be collaborasted with public systems for forwarding classification data  How to make live filtering systems after a request by a client such that any filter is applied before TCP session is setup or real data  How to make shared libraries between operating systems for access to classifications  How to access dns traffic in Mac and IOS systems  Minimalist approaches to filtering to reduce cpu load  Active filter lists that are only associated with real traffic seen from client  How to recognise the source of web-based DNS queries, and how to handle real-time DNS browser filtering within the Manifest V3 framework. | | |
| **How did the company determine that the outcome could not be known in advance?**   * There was no applicable information in scientific, technical, or professional literature or patents:   + True * Experts in the field provided advice that there wasn’t a solution that could be applied:   + True * There wasn’t a way to adapt solutions from other companies in, and out of, Australia:   + True | | |
| **Please explain what sources were investigated, what information was found, and why a competent professional could not have known or determined the outcome in advance (i.e. technical unknowns). (50 – 1,000 characters):**  Design Networks investigated research papers, industry articles, and documentation related to network security, ZTAs, DNS filtering, and IP filtering. It was determined that a competent professional may have been able to determine the outcome in advance to some extent, but there were technical unknowns related to the integration with the security DNS.  The state of knowledge existing prior to the activity provided a general framework for designing and implementing a ZTA, but did not provide a detailed solution that integrated seamlessly with Design Networks’ DNS and IP filtering. The technical unknowns included issues related to the integration of the client software with the security DNS, potential performance issues with DNS lookups, and potential challenges related to user experience and adoption. Therefore, conducting experimental R&D to design, develop, and test the ZTA with DNS and IP filtering was necessary to generate new knowledge and address the technical unknowns.  Technological unknowns relevant to FY23 include… and research conducted to seek to identify the existing state of knowledge and resolve these unknowns includes… | | |
| **What was the experiment and how did it test the hypothesis? (50 – 4,000 characters):**  Work undertaken in FY23 involved the following:   * Development of a stand-alone Windows system for managing DNS filtering employing the DNS resolver * Incorporation of the stand-alone system into a Windows-based ZTA framework * Conducting testing using the above models   Key variables include:   * Use of Design Networks’ DNS (see Core Activity 1 – developed in parallel with this activity); * Design of logic and modifications to endpoint software; * Ability for ZTA and DNS filtering functionality to work together; * DNS performance; * Overall network security. | | |
| **How did you evaluate or plan to evaluate results from your experiment? (50 – 4,000 characters):**  Evaluations of test results included:  For each endpoint, a series of manual tests were conducted to ensure:   * + DNS and IP filtering rules were being implemented as expected;   + Zero-Trust functionality was not affected.   Test ZTAs were created to host each of the endpoints, and traffic and availability of each endpoint was monitored. Each time an endpoint failed or was not available, an error was raised, and the issue investigated.  The company observed the following in FY23:   * What test results did you get? What technical issues, failures or challenges occurred? * What modifications did you make in response to the technical challenges? * What was the result of these tests / modifications – i.e. was the design successful or will further changes be required? | | |
| **Describe the conclusions reached from your experiments in the selected income period. (50 – 4,000 characters):**  As of 30 June 2023, the hypothesis was proven, in that the new code was successfully able to demonstrate that the DNS filtering could work within a ZTA framework, and that it was possible to incorporate a stand-alone system with minimal modifications.  In future financial year**s the development of client-facing code and reporting systems would need to be examined, and in particular more work would need to be conducted on potential scalability and performance concerns.** | | |

|  |  |  |
| --- | --- | --- |
| Core Activities Description | | |
| Core Activity 3: Design, development and testing of a methodology for redirecting browser users to render a blocked site on a remote secure rendering service | Start date:  Jul 2021 | End date:  Jun 2023 |
| **What was the hypothesis? (50 – 4,000 characters):**  While internet access always carries some degree of risk, there are lists of IP addresses and domain names that can identify high-risk websites. However, it is often difficult to advise or stop a user from accessing a dangerous website, as the web request is typically encrypted through HTTPS. A Man-in-the-middle (MITM) attack is where a malicious actor or logic is positioned between a user and an application, and impersonates one of the parties, making it appear as if a normal exchange of information is underway. The attack allows secret information (such as usernames or passwords) to be extracted from the network traffic. MITM techniques may break security protocols and be stopped as techniques become generally known, while shared key methods can expose trusted communications to end-users, which is generally not desirable.  It is hypothesised that, to address this issue, a technique using a web plug-in for a browser, possibly shared between multiple browsers, can be developed to allow checking of a URL's risk level before accessing it. Additionally, if a site is deemed dangerous, redirection to a renderer can be employed to display the page safely. The task is to combine URL access, risk checking, and redirection to ensure safe browsing practices while maintaining end-user privacy and security. By implementing such a system, users and organizations can more effectively manage risk and minimize the potential for harmful website access.  The success of this development is determined via the following:   * The ability to access the web address must not delay the process by > 250ms; * The testing of the URL must be completed with 500ms on average and never > 1.5secs; * The authentication process must not delay the request by > 500ms and only be applied at the first request or after an hour; * The render must give indications that it is being used and respond within 5 secs of the request.   In the first year work focussed on developing and producing a database and access method with basic tools to test and evaluate speed and reliability of data. All results showed significant opportunity for the approach to scale and provide considerable value for client software. The second year we have focused on how to use the data with clients in Windows, Linux, Unix (BSD PfSense). | | |
| **Did you conduct this core activity for a substantial purpose of generating new knowledge?**  Yes.  *(Populated by default - a core activity must be conducted for at least a substantial purpose of generating new knowledge.)* | | |
| **What new knowledge was this core activity intended to produce? (50 – 1,000 characters):**  New knowledge is generated in the form of a system to prompt the remote render of a site, to avoid MITM alerts. The approach allows for a consolidation of function in a single client, separates between the environment for management and data flow, enables a common logging system for all actions, focuses functionality on the client software, adds to the security of the services, and adds functionality to the client.  Additional new knowledge sought to be generated from experimentation conducted in FY23 includes the extent by which browsers working under Manifest V2 and Manifest V3 are able to intercept URLs prior to content being downloaded and a computer being put at risk; if it is possible to confirm the safety or otherwise of URLs prior to downloading; and if the approach used in Manifest V2 can subsequently be incorporated into Manifest V3. If the answer to Manifest V2’s conversion to Manifest V3 was no, alternative solutions would be developed such that the same level of protection could be provided within the Manifest V3 framework using alternative approaches. | | |
| **How did the company determine that the outcome could not be known in advance?**   * There was no applicable information in scientific, technical, or professional literature or patents:   + True * Experts in the field provided advice that there wasn’t a solution that could be applied:   + True * There wasn’t a way to adapt solutions from other companies in, and out of, Australia:   + True | | |
| **Please explain what sources were investigated, what information was found, and why a competent professional could not have known or determined the outcome in advance (i.e. technical unknowns). (50 – 1,000 characters):**  In conducting the activity related to the hypothesis, the key technical challenges were identified as developing a standalone solution for checking the risk level of a website, integrating this solution with other security protocols, and ensuring usability for clients. Before commencing the activity, research was conducted on current internet standards, DNS RFC, and code used by major ISPs and Google, as well as approaches to adding services to web browsers and API approaches for authentication, encryption, authorization, and user identification. Although some MITM techniques were found in the existing state of knowledge, there was no fully functional solution for clients. The state of knowledge did not allow for the development of a complete solution due to the complexity of integrating multiple protocols and ensuring usability for clients, and thus experimental R&D was necessary to test the hypothesis and generate new knowledge.  Technological unknowns relevant to FY23 include… and research conducted to seek to identify the existing state of knowledge and resolve these unknowns includes… | | |
| **What was the experiment and how did it test the hypothesis? (50 – 4,000 characters):**  Work undertaken in FY23 involved the following:   * Development of both Manifest V2 and Manifest V3 plugins to capture and check URLs prior to downloading * Development of an algorithm to redirect malicious URLs to warning pages * Integration of the Manifest V3 plugin with an external stand-along DNS resolver with or without a ZTA framework * Conducting testing of the above in multiple browser/operating system configurations and with both top level and internal domain requests.   Key variables include:   * Design of logic behind the plug-in; * Efficacy of the plug-in in prompting remote rendering; * Efficacy of the plug-in in avoiding the MITM warning; * Performance. | | |
| **How did you evaluate or plan to evaluate results from your experiment? (50 – 4,000 characters):**  Design Networks conducted various tests to ensure the effectiveness and efficiency of the solution. The tests include checking the success rate of blocking bad websites, authentication of authorized users, denying access to unauthorized users, testing the ZTA against multiple sites, identifying ZTAs and Internet traffic, testing the response time for handling large loads of Internet traffic, and testing the white list/black list functionality.  The company observed the following in FY23:   * What test results did you get? What technical issues, failures or challenges occurred? * What modifications did you make in response to the technical challenges? * What was the result of these tests / modifications – i.e. was the design successful or will further changes be required? | | |
| **Describe the conclusions reached from your experiments in the selected income period. (50 – 4,000 characters):**  As of 30 June 2023, the hypothesis was proven. It was possible to capture, check and redirect URLs under Manifest V2 in real time with no significant impact on user experience.  It was also possible to integrate a stand-alone DNS resolver to provide the same functionality in Manifest V3, in spite of the changes to the new framework.  In future financial years, load and scalability testing would be required, as would testing on mobile devices. | | |

|  |  |  |
| --- | --- | --- |
| Core Activities Description | | |
| Core Activity 4: … (max 200 characters) | Start date:  Jul 2022 | End date:  Jun 2023 |
| **What was the hypothesis? (50 – 4,000 characters):**  It is hypothesised that the company can develop or progress XX technology/method to create or enhance YY product to achieve ZZ outcome/benefit OR to overcome specific issues identified with existing comparable solutions. | | |
| **Did you conduct this core activity for a substantial purpose of generating new knowledge?**  Yes.  *(Populated by default - a core activity must be conducted for at least a substantial purpose of generating new knowledge.)* | | |
| **What new knowledge was this core activity intended to produce? (50 – 1,000 characters):**  New knowledge is generated in the form of … that can improve/achieve …  Existing solutions have limitations…  Alternate technologies/processes used in other industries could not be easily adapted, using known principles, due to… | | |
| **How did the company determine that the outcome could not be known in advance?**   * There was no applicable information in scientific, technical, or professional literature or patents:   + True or false; * Experts in the field provided advice that there wasn’t a solution that could be applied:   + True or false; * There wasn’t a way to adapt solutions from other companies in, and out of, Australia:   + True or false. | | |
| **Please explain what sources were investigated, what information was found, and why a competent professional could not have known or determined the outcome in advance (i.e. technical unknowns). (50 – 1,000 characters):**  Please explain:   * What are the key technical challenges or uncertainties relevant to your hypothesis; * What process you went through in relation to searching for relevant knowledge before activity commencement (e.g., research via google/journals, engagement and consultation with industry experts, etc.); * Details of what was found in respect of the state of knowledge existing prior to commencement of your activity based on your search; * Why the state of knowledge existing prior to commencement of your activity did not allow you to determine the outcome of your hypothesis in advance. This must explain why you needed to generate new knowledge by conducting experimental R&D to test your hypothesis. | | |
| **What was the experiment and how did it test the hypothesis? (50 – 4,000 characters):**  A systematic progression of design and testing was undertaken, which involved the following:   * Development of… * Conducting testing…   Key variables include:   * E.g. design of the system (i.e. what you are changing) * E.g. environmental factors * E.g. speed / accuracy / efficiency (i.e. what you are testing for) | | |
| **How did you evaluate or plan to evaluate results from your experiment? (50 – 4,000 characters):**  Evaluations of test results included:  Test results were evaluated through a process of…  The company observed the following:   * Iteration 1 investigated … design idea. Testing found it would achieve… result which did not achieve the hypothesis. * Iteration 2 involved redesigning … to … in an attempt to overcome the issues identified in iteration 1. Testing of this design found that… * Iteration 3 comprised of redesigning… and adding… in an attempt to overcome the issues identified in iteration 2. Testing of the new design found…   OR   * What test results did you get? What technical issues, failures or challenges occurred? * What modifications did you make in response to the technical challenges? * What was the result of these tests / modifications – i.e. was the design successful or will further changes be required? | | |
| **Describe the conclusions reached from your experiments in the selected income period. (50 – 4,000 characters):**  As of 30 June 2023, the hypothesis was / was not proven …  In future financial years… | | |

|  |  |  |
| --- | --- | --- |
| Supporting Activities Description | | |
| Supporting Activity 1: Background research and project management | Start date:  Jul 2021 | End date:  Jun 2023 |
| **Briefly describe this supporting activity. (50 – 1,000 characters):**  The following activities were undertaken in support of the Core Activities:   * Literature search and review; * Analysis of previous design solutions and assessment of key interferences to determine potential solutions; * Consultation with industry experts; * Project management relevant to facilitating R&D activity (e.g. record management and administration directly related to conducting the experiments). | | |
| **How did this activity directly support the core activities? (50 – 1,000 characters):**  The background research activity is directly related to the Core Activities as it allows the company to determine whether the outcome could be known in advance, via literature reviews and consultations with industry professionals, and thus whether new knowledge will be generated via the undertaking of the experiments outlined within the core activity. Information and knowledge found from this background research and project management is used as evidence that the specific technology to be designed does not yet exist and for further development of the core hypotheses. | | |
| Relationship with Core Activities | Directly related to all core activities | |
| Did this activity produce a good or a service, or is it directly related to producing a good or a service? | No | |
| If yes above, was this activity undertaken for the dominant purpose of supporting the core activity (must be yes)? | NA | |

|  |  |  |
| --- | --- | --- |
| Supporting Activities Description | | |
| Supporting Activity 2: Software integrations and background development | Start date:  Jul 2021 | End date:  Jun 2023 |
| **Briefly describe this supporting activity. (50 – 1,000 characters):**  The following activities have been undertaken in support of the Core Activities:   * Development and testing of a test API authentication; * Develop a DNS model with basic extended features, and testing over HTTPs for extended data services. | | |
| **How did this activity directly support the core activities? (50 – 1000 characters):**  This work is necessary to facilitate the development, testing and use of the core developments. | | |
| Relationship with Core Activities | Directly related to all Core Activities | |
| Did this activity produce a good or a service, or is it directly related to producing a good or a service? | No | |
| If yes above, was this activity undertaken for the dominant purpose of supporting the core activity (must be yes)? | NA | |

# Estimate of Total Project Cost Allocated to Each Registered Activity

|  |  |
| --- | --- |
| Activity  (i.e. time/cost spent on each activity) | Estimate of Proportion of Effort/Expenditure  (Please estimate the split of effort of the above nominated activities against each other) |
| Core Activity 1: Design, development and testing of a DNS filtering service | 30% |
| Core Activity 2: Design, development and testing of a Zero-Trust architecture with DNS and IP filtering of external connections | 30% |
| Core Activity 3: Design, development and testing of a methodology for redirecting browser users to render a blocked site on a remote secure rendering service | 30% |
| Core Activity 4: … (if relevant) | XX% |
| Supporting Activity 1: Background research and project management | 6% |
| Supporting Activity 2: Software integrations and background development | 4% |
| **Total** | **Must sum to 100%** |

# Substantiation

Please be aware that, under the current legislation, you must be able to provide evidence to substantiate your R&D activities. In the event of an AusIndustry audit, this documentation may be required to prove that the R&D activities were eligible and took place in a systematic progression of work. We strongly recommend that you store this evidence in a safe place.

Please confirm which of the following documents you have available.

You do not need to send us any of these documents.

|  |  |
| --- | --- |
| Yes / No | Type of substantiation |
| Yes | Evidence of searches or enquiries you made to find current knowledge |
| Yes | Evidence to show that you could only determine the outcome of the core activity by conducting experiments as part of a systematic progression of work |
| Yes | Evidence of your hypothesis and design of your experiments |
| Yes | Documented results and evaluation of your experiments |
| No | Other (if yes, please describe) |