Security Standard – Firewall Security (SS-013)

Chief Security Office

Date: 18th December 2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

1. Introduction

1.1. This Firewall Security Standard provides the list of controls that are required to secure firewall implementations to a Department of Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data filtered by firewalls. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from the international best practice for firewall security and have been tailored for Departmental suitability in accordance with the DWP Firewall Policy.

1.4. This document primarily covers Layer 4 / packet filtering firewalls, but it is recognised that more modern firewall capabilities (Layer 7 or application firewalls) are being introduced into the Department, such as policy enforcement based on packet inspection i.e. firewalling which HTTP commands can be used, scanning for malware etc. This document will be updated to reflect this in future iterations as more information becomes available.

1.5. This document describes the standards for both physical and virtual firewalls, e.g. physical interfaces being configured as VLAN trunks to expose virtual interfaces, although additional controls may be required to enforce security boundaries in virtualised systems.

1.6. This document does not mandate any particular firewall manufacturer over another – the DWP estate is large and complex and a number of different manufacturer's firewalls have been deployed. The Technology Radars (and security architects if necessary) should be consulted for guidance on product choice, but the focus should be on capability and suitability to meet requirements. It should also be noted that open source products may also be considered, again with the focus on meeting requirements.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for secure firewall deployments.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

3. Exceptions

3.1. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.3. Exceptions to this standard MUST be maintained on the project risk register for accountability, traceability and security governance reporting to senior management. As and when the GRC tool is implemented, these risks will also be identified centrally.

4. Audience

4.1. This standard is intended for DWP IT staff and its suppliers, involved in securing firewalls for DWP systems and provides the security requirements on how to secure them.

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP), including the handling caveat OFFICIAL-SENSITIVE. All of the organisation's firewall implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all firewall systems that are provisioned for departmental use.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section 3. Exceptions above).

8. Firewall Change Management Plan

Firewall changes are a necessary ongoing process that ensures firewall rules are continuously capable of preventing security breaches. A well-defined management plan MUST include the following:

Reference	Security Control Requirement
11.1	A detailed plan of changes and their objectives
11.2	An estimation of risks due to the policy changes, their expected impacts, and a mitigation plan
11.3	A centralised change-management workflow and change-control policy between different network teams and proper change approvals, authorised by a suitably empowered individual that includes an assessment of the rule changes against the live service.
11.4	Proper audit trails of the change including who made the change, when they made it, and the outcome of the change

9. Test Firewall Policy and Rule Changes

Any planned policy or rule changes MUST be tested prior to committing to a change to avoid unexpected detriment to the network. The following steps MUST be taken to test Firewall policy and rule changes:

Reference	Security Control Requirement
12.1	Trace the path of packet traversal through the network layer and confirm that all devices along the path allow the packet to reach its intended destination
12.2	Confirm that the firewall is allowing and blocking data according to the established policies and rule sets
12.3	Perform an analysis to identify which device policies or rules are blocking the packet from reaching its destination
12.4	Where feasible, the policy or rule changes should be tested in a suitable non-production environment before being pushed to the active live environment. Where this is not feasible and the change has to be applied to the active live environment, the change must not be closed down until the policy / rules have been tested and validated to work as expected. Where testing fails, back-out should be made to a previous version of the policy / ruleset.

10. Firewall Rule Management

Firewall rule management is a critical activity. Without effective rule management there might be many firewall rules, objects redundancies, duplicate rules, and bloated rules that can negatively affect firewall security, performance and efficiency. Going forwards, firewall rule management will become part of the Continuous Integration Pipeline as DWP maturity in this area grows.

Reference	Security Control Requirement
13.1	Redundant or duplicate rules MUST be removed as they slow firewall performance due to processing more rules in sequence
13.2	Orphaned or unused rules MUST be removed as they complicate rule management - Project decommissioning must remove any associated firewall rules.
13.3	Be mindful of shadowed rules as they can leave any other critical rules unimplemented i.e. a broader rule matching a set of criteria is configured above a more specific rule.
13.4	Conflicting rules MUST be amended as they may create backdoor entry points
13.5	Be mindful of erroneous or incorrect rules with typographical or specification inaccuracies as they can cause rules to malfunction - All rules and changes to rules must be quality assured by an independent person to remove typos and errors before being implemented.
13.6	All rules and objects SHOULD use naming conventions that make the rule base easy to understand. For example, use a consistent format such as host name IP for hosts. Where a firewall is shared amongst multiple projects/products, consider including a reference to the service name/code in a firewall change log to help keep track of which rule belongs to who. All rule changes MUST contain a valid change reference so that they can be tracked back to the change record and approver.
13.7	Rules MUST be prioritised in proper logical order to ensure that the firewall processes them according to the security requirements of the firewall policy. Always place more specific rules first and general rules last
13.8	Rules that belong together MUST be grouped
13.9	You SHOULD not use ANY in port number, source or destination address except by authorised exception. You MUST never create an ANY, ANY, ANY or equivalent ALLOW ALL rule, as this may result in allowing every service through the firewall.
13.10	Any rules that can't be assigned to a known product, project or service owner should be monitored for traffic for 30 days. If traffic is not detected the rule should be disabled and left in place for a minimum of 14 calendar months. If after this time a request is not made to re-enable the rule it should be removed and the change logged.
13.11	Any objects that define multiple networks should be reviewed at least annually, to ensure they remain valid.
13.12	Expiry dates MUST be added to temporary rules and reviewed at least annually for rule clean-up
13.13	Any significant project change should include a review of its associated firewall rules
13.14	The entire firewall ruleset should be reviewed at least annually to confirm alignment with the standard, remove defunct rules, as an audit function, and to identify any vulnerable rules.
13.15	If the firewall supports notes or in-rule documentation, extensive use should be made of it

11. Firewall Security Audits

Firewall policy audits are necessary to ensure that firewall rules are compliant with organisational security regulations as well as any external compliance regulations that apply.

Reference	Security Control Requirement
14.1	A firewall security audit MUST take place when a new firewall is installed, and annually thereafter.
14.2	A firewall security audit MUST take place when firewall migration activity is occurring on the network
14.3	A firewall security audit MUST take place when there is bulk configuration changes made on firewalls
14.4	If supported, rule-counters should be used to determine how often a rule has been used.

12. Firewall User Access and Authorisation

It is important to institute stringent network-access security and user-permission control to ensure that only authorised administrators have access to change firewall rules.

Reference	Security Control Requirement
15.1	Where possible, network configuration management techniques should be adopted to monitor firewall configuration changes in real time and provide alerts if there are unwarranted configuration changes
15.2	There MUST be a configuration restore option in place when unexpected or incorrect configuration changes have been made on the firewall and you need to revert back to an earlier state. To support this, backups of the firewall configuration MUST be taken every time a change is made, with at least 10 backups being kept for analysis should the need arise.
15.3	Firewall logs MUST be monitored to identify any unauthorised break-in attempt on the firewall from both inside and outside the network – the DWP Security Operations Centre will perform monitoring and analysis via a SIEM tool on both general firewall use and also for administrative change. Firewall logs should be sent to the SIEM tool via a secured protocol.
15.4	Users in charge of managing firewalls MUST do so via individual administrative accounts provisioned for that purpose, managed on a centralised basis, and authenticated using an appropriate protocol, such as RADIUS, TACACS or LDAP. No firewall changes beyond initial configuration required to enable a secure authenticated connection should be performed using local accounts. Local accounts may exist for use in emergencies only, but these must be appropriately secured and their use audited.
15.5	All firewall management MUST be conducted from a dedicated management network that maintains separation from other network security domains.

13. Firewall Ingress and Egress Traffic Filtering

Egress traffic filtering is required to help mitigate the threat of data exfiltration.
Ingress traffic filtering is required to help mitigate the threat of malware, spoofing and denial-of-service attacks.
This can refer to firewalls separating a higher security domain from a lower one, but can also refer to separation between two equal level domains.

Reference	Security Control Requirement
16.1	IP spoofing MUST be blocked.
16.2	You MUST only allow ingress connections from approved and risk assessed end points.
16.3	Outbound traffic from VLAN workgroups or entire network segments that have no need establishing client connections to internet servers MUST be dropped.
16.4	Broadcast traffic MUST be dropped unless an exception is made (please refer to section [6. Exceptions] above)
16.5	All unauthorised traffic should be blocked from entering or leaving the firewall boundary.
16.6	Outbound traffic with destinations that are listed on DROP filter lists MUST be dropped. Similarly, inbound traffic from such destinations MUST also be dropped.
16.7	Only allow client hosts to access authorised services from authorised external servers (NIST-800-53R4 Access Controls AC-4 (17))
16.8	For inter-server communications involving external servers, only allow access to service ports your internal servers must use to operate correctly. Care needs to be taken regarding ports on a Windows server that are not normally permitted through a firewall.
16.9	Block routing protocols at the firewall - firewalls should not perform dynamic routing. Static routes only.
16.10	If DNS is provided internally, or uses a split DNS, use internal resolvers as forwarders for the internal networks
16.11	If an HTTP proxy, or a proxy system that performs web URL or content filtering is deployed, only allow outbound client web connections through the firewall via the proxy/proxies
16.12	If services are authorised that make use of unique ports for remote desktop, subscription, or licensing channels, only allow access to these services from hosts that are authorised to use them
16.13	Firewalls should silently drop packets and never reject them i.e. never send a TCP RST or ICMP destination unreachable and acknowledge the device’s existence.
16.14	Implement rate limiting on ingress traffic to mitigate against Denial of Service attacks.

14. Firewall Patching and Updates

Vendors release firewall upgrades and version updates for many security reasons, importantly some are to combat vulnerabilities and loopholes in outdated hardware and software.

Reference	Security Control Requirement
17.1	You MUST patch the firewall's operating system and application software with the latest security patch on an N-1 version of the code base at least every six months, or in response to a risk raised through vulnerability management.
17.2	Vulnerability tests MUST be conducted on firewalls to assess hardware or software for flaws and weaknesses – internet facing firewalls MUST have a full ITHC at least annually.

15. Additional Firewall Best Practices

The following controls are additional requirements to consider to ensure firewalls are configured for optimal effectiveness.

Reference	Security Control Requirement
18.1	You MUST change the default firewall administrator or root password – please refer to the Password Management Access Control Standard to identify password minimum requirements.
18.2	For physical firewalls, you MUST ensure that physical access to the firewall is controlled as per the DWP Physical Security Policy
18.3	You MUST enable firewall AND rule logging and alerting.
18.4	You MUST use a secure remote syslog server and a secured protocol that makes log modification and manipulation more difficult for a malicious attacker
18.5	You MUST backup the firewall rulebase and configuration files at least every 6 months, AND before and after any changes are made.
18.6	Firewalls MUST be implemented and configured to operate resiliently in case of hardware or physical environment failures
18.7	Firewalls must synchronise to a central DWP time source

16. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	When the next ITHC is performed on the application in question.

17. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

18. Security Standards Reference List

Document Name	Location	Version
Exceptions Process	XX/XX/XX	
DWP Physical Security Policy		
DWP Firewall Policy	Link to be added once published	1.0

19. Reference Documents

DWP Digital Blueprint

Cdn.swcdn.net (2013) *Best Practices for Effective Firewall Management* [online] 22nd October 2013. Available from: http://cdn.swcdn.net/creative/v9.3/pdf/Whitepapers/Best_Practices_for_Effective_Firewall_Management.pdf. [Accessed: 6th February 2017]

Principlelogic.com (2009) *Firewall Best Practices* [online] 12th May 2009. Available from: https://www.principlelogic.com/docs/Firewall_Best_Practices.pdf [Accessed: 3rd February 2017]

Securityskeptic.com (2014) *Firewall Best Practices – Egress Traffic Filtering* [online]. Available from: http://securityskeptic.typepad.com/the-security-skeptic/firewall-best-practices-egress-traffic-filtering.html. [Accessed: 10th February 2017]

20. Glossary

Abbreviation	Definition
BGP	Border Gateway Protocol
CPU	Central Processing Unit
DA	Design Authority
DNS	Domain Name System
DWP	Department of Work and Pensions
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
SIEM	Security Incident and Event Management

Abbreviation	Definition
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network

21. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the control points in DWP's baseline control set.

SS-13 Security Standard Control	Baseline Control Set
11.1	ISO 27002: 12.1.2.a
	NIST 800-53: CM-3c
	OWASP ASVS: x
11.2	ISO 27002: 12.1.2.c
	NIST 800-53: CM-3b
	OWASP ASVS: x
11.3	ISO 27002: 12.1.2.d
	NIST 800-53: CM-3g
	OWASP ASVS: x
11.4	ISO 27002: 12.1.2.a
	NIST 800-53: CM-3f
	OWASP ASVS: x
12.1	ISO 27002: 12.1.2.b
	NIST 800-53: CM-3 (2)
	OWASP ASVS: x
12.2	ISO 27002: 12.1.2.b
	NIST 800-53: CM-3 (2)
	OWASP ASVS: x
12.3	ISO 27002: 12.1.2.b
	NIST 800-53: CM-3 (2)
	OWASP ASVS: x
13.1	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.2	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.3	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.4	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.5	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.6	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.7	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.8	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-13 Security Standard Control	Baseline Control Set
	OWASP ASVS: x
13.9	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.10	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.11	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
13.12	ISO 27002: 13.1.1.c
	NIST 800-53: CM-6
	OWASP ASVS: x
14.1	ISO 27002: 18.2.3
	NIST 800-53: AU-2
	OWASP ASVS: x
14.2	ISO 27002: 18.2.3
	NIST 800-53: AU-2
	OWASP ASVS: x
14.3	ISO 27002: 18.2.3
	NIST 800-53: AU-2
	OWASP ASVS: x
15.1	ISO 27002: 12.1.2
	NIST 800-53: CM-3 (5)
	OWASP ASVS: x
15.2	ISO 27002: 12.1.2.g
	NIST 800-53: CM-2 (3)
	OWASP ASVS: x
15.3	ISO 27002: 12.4.1
	NIST 800-53:
	OWASP ASVS: x
15.4	ISO 27002: 9.2.3.b
	NIST 800-53: AC-6
	OWASP ASVS: x
16.1	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.2	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.3	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.4	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.5	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.6	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.7	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4 (17)
	OWASP ASVS: x

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-13 Security Standard Control	Baseline Control Set
16.8	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.9	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.10	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.11	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.12	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
16.13	ISO 27002: 13.1.1.c
	NIST 800-53: AC-4
	OWASP ASVS: x
17.1	ISO 27002: 12.6.1
	NIST 800-53:
	OWASP ASVS: x
17.2	ISO 27002: 12.6.1
	NIST 800-53:
	OWASP ASVS: x
17.3	ISO 27002: 12.5.1
	NIST 800-53:
	OWASP ASVS: x
18.1	ISO 27002: 12.1.3
	NIST 800-53:
	OWASP ASVS: x
18.2	ISO 27002: 9.2.1.a
	NIST 800-53:
	OWASP ASVS: x
18.3	ISO 27002: 9.4.3
	NIST 800-53:
	OWASP ASVS: x
18.4	ISO 27002: 11.1.2.b
	NIST 800-53:
	OWASP ASVS: x
18.5	ISO 27002: 12.4.1
	NIST 800-53:
	OWASP ASVS: x
18.6	ISO 27002: 12.4.2.b
	NIST 800-53:
	OWASP ASVS: x
18.7	ISO 27002: 13.2.1
	NIST 800-53:
	OWASP ASVS: x
18.8	ISO 27002: 12.3.1
	NIST 800-53:
	OWASP ASVS: x