GOV.UK

Guidance

Government network policy changes

Updated 13 March 2017

Contents

Print this page

This publication is available at https://www.gov.uk/government/publications/government-network-policy-changes/government-network-policy-changes

Foreword

The Public Services Network (PSN) provides technical policies regarding the operation of its network. At the Technology Leaders Network (TLN) a set of high level policies were agreed that provide high level guidance and ambition for the way in which government networks as a whole will be managed.

These policies do not have a specific timeframe for implementation in order to enable network service providers and customers to understand the implications and to aid future planning.

Email feedback to psnservicedesk@digital.cabinet-office.gov.uk.

Objectives of technical policy changes

The agreed policies aim to create a simpler, clearer mechanism for managing network services in government. The intention is not to force compliance to a new regime but rather to create the freedom to meet current and future demands. The objectives of the policies are to:

- operate the PSN as a single OFFICIAL network enabling services to be consumed from both the Assured and Protected networks
- enable the use of cloud email services that meet specific security standards for government email
- bring PSN and other government DNS services into line with best practice by allowing government DNS records, including records currently on PSN servers, to be hosted outside the PSN

Technical network policy statements

1.Network routing between PSN Assured and PSN Protected

Government has previously seen PSN as 2 distinct shared networks supporting separate security classifications. Following changes to the Government Security Classifications (https://www.gov.uk/government/publications/government-security-classifications) and consultation with government customers, we must no longer treat these as 2 networks. Instead, the PSN must be seen as a single shared network to transmit data classified OFFICIAL. In particular:

1. A PSN direct network service provider (DNSP) that operates both Protected and Assured networks can route directly between the Protected and Assured networks without restriction.
2. A DNSP can route from a customer it has on the Assured network to a customer running on another DNSPs Protected network.
3. The DNSP does not need to send traffic via the Vodafone gateway service (SRV_0049) to pass between the Protected and Assured networks, but can continue to use this gateway if it chooses to.

A shared cross-PSN encryption overlay, PSN Protected, is available to encrypt data in transit at the network layer if customers need it. To avoid routing issues, all IP addresses (https://www.gov.uk/guidance/how-to-connect-and-configure-your-systems-to-the-public-services-network-psn#ip-addresses-reachable-on-psn) used for this overlay must be different from those used for PSN Assured.

This policy gives customers the opportunity to review and rationalise their connections. When deciding whether to connect via PSN Assured or PSN Protected, organisations should consider:

- the network principles (https://www.gov.uk/government/publications/network-principles/network-principles)
- where they send most of their traffic
- where they receive most of their traffic from
- that any traffic that needs to transit from PSN Protected to PSN Assured means recipient organisations on PSN Assured have to pay to use a gateway between PSN Protected and PSN Assured

DNSPs may need to share information with each other to ensure that any large step-changes in traffic between PSN Assured and PSN Protected don't impact customers. The PSN team will facilitate this.

2.DNS

a. All RIPE IP addresses that are reachable via the PSN, and the information stored in the DNS about these IP addresses, is classified as OFFICIAL. As a result of this, PSN IP addresses can be published on public DNS servers.

b. Government organisations must put mechanisms in place to protect and detect the integrity of DNS records used for government services.

3.Email

a. Email communications between central government organisations external to the PSN must be encrypted in transit.

b. Central government organisations must have technical and business policy in place to ensure the sender or recipient of government email can be verified.

Print this page