GARRISON

Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice: Privileged Access and "Browse Down"

The Electronic Communications (Security Measures) Regulations 2022 and the Telecommunications Security Code of Practice explicitly require UK Telecommunications Service Providers (and their suppliers) to replace existing "Bastion Host" or "Jump Box" approaches to securing privileged access with a "Browse Down" model. Garrison provides an NCSC-assured "Browse Down" technology which can be provided either as an on-premises technology or as a cloud service.

Regulatory requirements

Section 4.4(a) of the Electronic Communications (Security Measures) Regulations 2022 require network providers to "take such measures as are appropriate and proportionate":

To ensure that workstations through which it is possible to make significant changes to security critical functions are not exposed:

a) in the case of a public electronic communications network, to incoming signals,

b) in the case of a public electronic communications service, to signals that are incoming signals in relation to the public electronic communications network by means of which the service is provided, or

c) where, in either case, the workstation is operated remotely, to signals capable of being received by the workstation.

The Telecommunications Security Code of Practice (CoP) makes this requirement clearer and more explicit. In Figure 1, the CoP explicitly identifies as unacceptable the Browse Up security model that underpins the use of Bastion Hosts or Jump Boxes for privileged access to critical network functions:

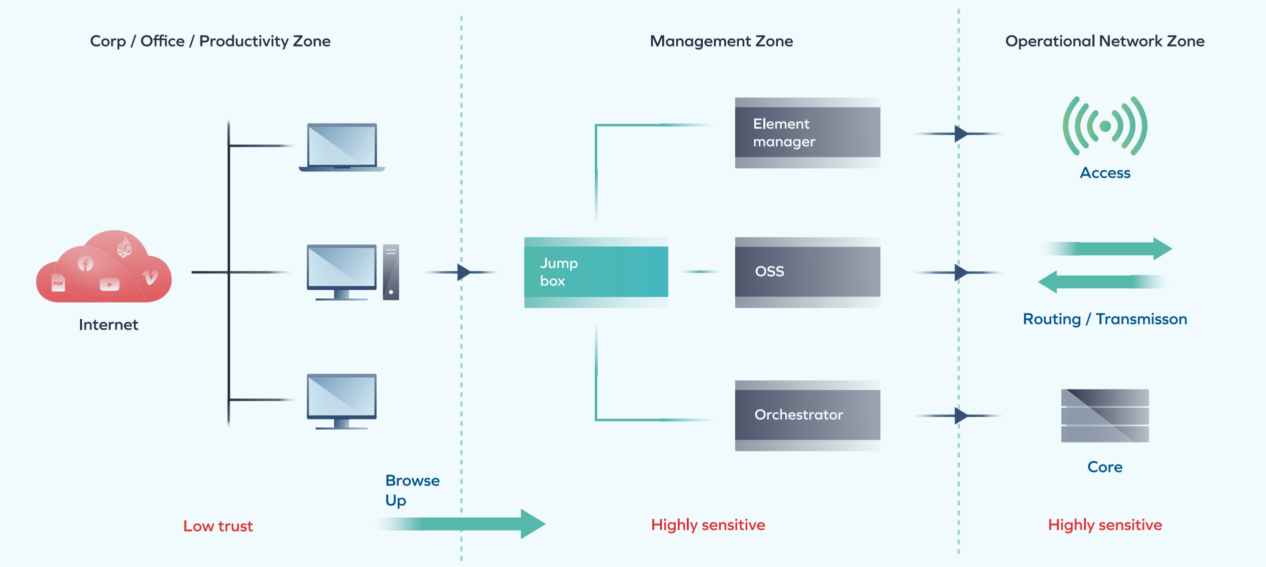


Figure 1. Example of Browse Up architecture

* Figure 1 reproduced from the Telecommunications Security Code of Practice
1 https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_3

GARRISON

Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice: Privileged Access and "Browse Down"

Neither the Regulations nor the CoP explicitly define Browse Down but on the National Cyber Security Centre (NCSC) website, Browse Down is defined as "when you trust your device just as much, or more, than the system you are administering"[2]. The NCSC website further provides "an example of a Browse Down pattern, where riskier activities are isolated using a separate processing context"[3].

As per the associated NCSC guidance[1] the regulations require that any such current deployments are replaced with an alternative Browse Down security model, as depicted in the CoP's Figure 2 below.

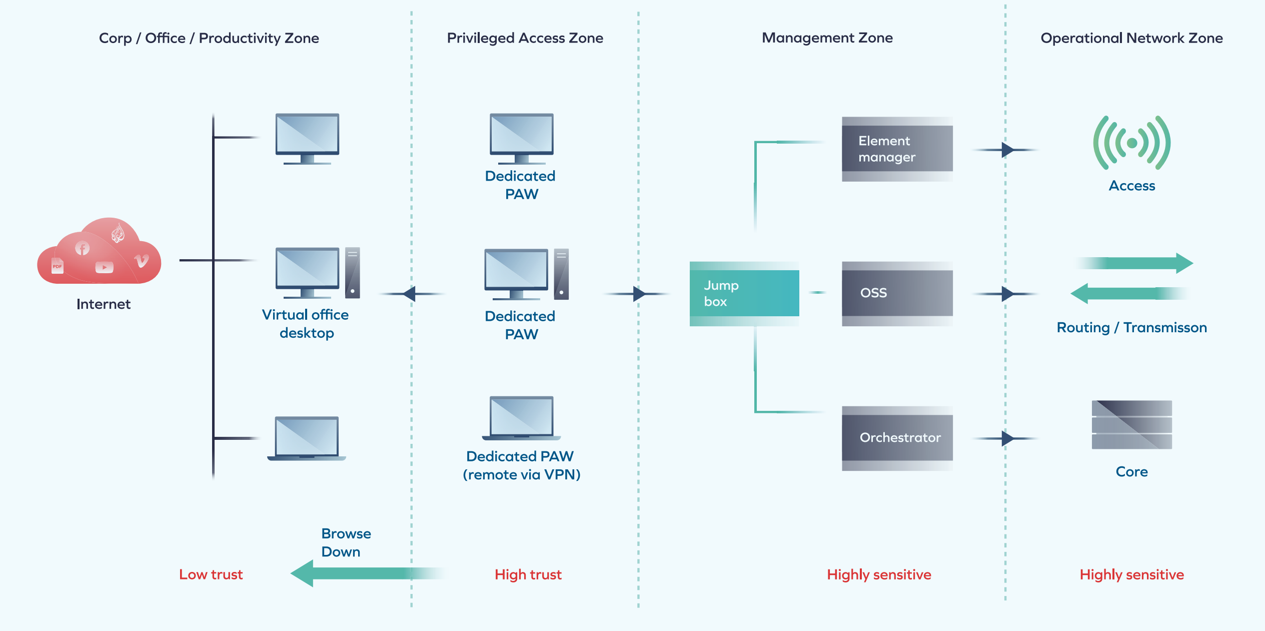


Figure 2. Example of Browse Down architecture

* Figure 2 reproduced from the Telecommunications Security Code of Practice

[2] https://www.ncsc.gov.uk/collection/secure-system-administration/gain-trust-in-your-management-devices

[3] https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech

GARRISON

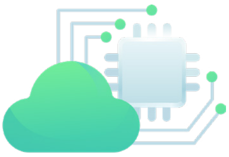
Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice: Privileged Access and "Browse Down"

Garrison's "Browse Down" solutions

Garrison supplies Browse Down technology to both commercial organisations such as Lloyds Banking Group[4] and to UK Government customers including the Ministry of Defence[5]. This technology has been extensively assessed by the NCSC, to the extent that it is trusted to provide Browse Down even from classified devices that wish to access the Internet. Garrison's Browse Down technology can be provided in two forms:

Garrison SAVI®

Garrison SAVI® is an on-premises Browse Down capability that consists of hardware appliances deployed into a customer's datacentre. Appliances are typically configured as a standard perimeter protection device, with a client interface connected to an "internal" network, and a Remote interface connected to a DMZ. Appliances can optionally be deployed behind a Secure Web Gateway in order to provide URL filtering to block access to inappropriate content and credential-stealing sites. In addition to its use for accessing untrusted websites, Garrison SAVI® can also be configured for Browse Down to untrusted VDI servers (for example, if users of Privileged Access Workstations need to access VDI servers owned and operated by an untrusted 3rd party).



Garrison ULTRA®

Garrison ULTRA® is a cloud service providing a true Browse Down capability using the same underlying technology as Garrison SAVI®. Garrison ULTRA® can be simply configured, with user authentication via SAML (or an alternative access-key approach if required). Garrison ULTRA® provides customer-configurable URL filtering to block access to inappropriate content and credential-stealing sites. In the commercial world, this approach, is referred to as Browser Isolation. However, unlike other commercial Browser Isolation solutions, Garrison ULTRA® is – under the covers – based around a true Browse Down technology.

Contact us at info@garrison.com for more information

[4] https://www.garrison.com/lloyds-banking-group
[5] https://www.garrison.com/cross-domain