Third Party Network Management Standard

Best practice

Issue 1.0
Date: 27/04/2016
Author: BT Security, 3rd Party Security Team

SEC/STD/BP003

Contents

1 Introduction

1.1 General

This document lays out the network management controls needed to secure networks and or network devices running open system interconnection (OSI) Layer 2 and 3 routing and switching functions.

1.2 Objectives

Inconsistent implementation of security requirements may result in vulnerabilities in network infrastructure. The principal objective of this document therefore is to provide a benchmark standard to ensure consistent and secure controls are implemented on third party networks by:

- only permitting access to authorised and registered users, at the minimum level required to perform their daily duties, in a way which ensures individuals are made accountable for their actions
- ensuring the confidentiality, availability and integrity of data transiting the network
- providing appropriate levels of security throughout the life of all such data, from creation to deletion
- allowing the monitoring of events performed by and on the network devices and data held on it
- enabling attempted violations to be identified and, if necessary, followed up in a timely and efficient manner
- meeting corporate and industry benchmark security requirements
- meeting any and all related legal and regulatory requirements
- ensuring a consistent approach to security on all networks and devices where this standard applies

The intended readership is Third parties in the BT Supply chain.

1.3 Document Structure

The structure of the document is that of a checklist, to allow implementers to record where they are, and are not, compliant with the standard. Here is a brief description of the columns included below:

Recommended Control: A description of the recommended standard.

Mechanism: What the standard states is the correct setting.

Reason for Control: The rationale for the control or consequences which might occur if the control is not implemented.

1.4 Additional Materials and Advice

UK Government (HMG) provides a high level advice sheet for protecting networks:

10 Steps to network security	https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-network-security--11

The Centre for the Protection of National Infrastructure (CPNI) also provides guidance on cyber protection, and includes sections on securing networks, such as:

Critical Security Controls Guidance	http://www.cpni.gov.uk/advice/cyber/Critical-controls/

2 Recommended Controls

2.1 Asset Management

Recommended Control	Mechanism	Reason For Control
Network devices should be included as part of an asset management policy.	The policy should allow for the following: • An up to date inventory/design that includes all network elements. • Classification of network assets and information they process. • Owners identified and recorded for all the network devices. • Definitions set around the acceptable use of network assets.	Without a clear record of assets it may be difficult to manage network devices. This could lead to misconfiguration and the introduction of vulnerabilities. Without a clear understanding of assets, incident response and recovery may also be affected.

2.2 Change Control & Update Procedures

Recommended Control	Mechanism	Reason For Control
Establish change control procedures	Document, implement, test, and follow a change control process for all additions, and alterations to network devices.	Changes made to devices without them firstly being adequately assessed, notified and authorised, could result in introducing security weaknesses.
Update procedure	In addition to the documentation and implementation of a change control procedure, an update process should also be documented and implemented.	Inadequate documentation of the update process could lead to misconfiguration and unavailability of a switch/router.

2.3 Network Security

Recommended Control	Mechanism	Reason For Control
When connecting a device or host to a network it is the responsibility of the equipment owner to ensure that authorisation to connect to the network has been granted by the network owner.	Any additions or changes to security gateways, including for support tool access, must be subject to an appropriate authorisation and change control process. The change control process should include a testing stage to ensure all changes work as expected.	Failure to operate a robust authorisation and change control process may lead to insecure systems connected to a network which could then be used by a remote attacker to launch attacks on the network and other systems connected to it.
Networks must be segregated into domains, and the criteria for interconnections between network domains must be defined.	Details of the network domains and interconnect policy should be documented with processes in place to enforce them. Documentation must be kept up to date and in line with the live network.	To minimise the risk of unauthorised access to systems, applications and network nodes within the defined security domain.
Connections to external networks	All connections to external networks must be made via a security gateway, where a device provides either open or filtered connectivity to the external networks. The security gateway must be able to hide the structure of the internal network and be capable of profiling users/traffic such that access times and permitted services can be defined and controlled. The router must be able to distinguish whether a packet comes from an external system by means of identifying which physical port a packet is delivered from. Note: This covers all types of application including technologies like VOIP.	To prevent unauthorised network access which could be exploited by a remote attacker.

Logical access to management ports must support two factor authentication. Where physical access measures are also required they must also support two factor authentication	Via: Smartcards, tokens, electronic access control with PIN	To prevent unauthorised access to and on the switch/router.
All unused network ports must be disabled	The minimum number of ports required for installation and commissioning should be enabled by default, all other ports should be administratively down/disabled.	To prevent unauthorised access to and on the switch/router.
Modem Connections	A modem must never be connected to the console or auxiliary port. This would bypass all security measures implemented within the trusted network (as well as allowing the determined hacker to perform password recovery remotely in the case of the console port).	To prevent unauthorised remote access to a switch/router.
It must be possible to validate all routing table entries	All routes must be documented in appropriate design documents and configurations either manually checked on a periodic basis or automatically checked by a configuration auditing tool.	To prevent vulnerabilities introduced through changed routing tables either maliciously or by accident.
Routing Protocols - security functionality which is available must be enabled by default	Any use of routing protocols which do not support security functionality or where it is not enabled should be documented with justification and any mitigations. Routing protocols must be mutually authenticated.	To prevent unauthorised access to and on the switch/router.

Routing between Autonomous Systems	All routing between Autonomous Systems (AS's) must be implemented using BGP (Border Gateway Protocol). BGP provides several advantages over static routes between domains i.e. policy can be applied both inbound and outbound, and preferred routing paths can be defined.	To prevent unauthorised access to the switch/router.
All systems must have their internal clocks synchronised to a trusted time source. Where this is not possible check clock synchronisation on a regular basis.	Reference Stratum 1 time sources. http://support.ntp.org/bin/view/Servers/StratumOneTimeServers	Failed transactions or inaccurate data could result where clock differences exist between systems.
Network monitoring tools	All functionality to capture or interrogate payload data must be disabled.	To prevent unauthorised use of network analysing & monitoring tools in order to gain information about the network or data transmitted across it, in order to attack the system or network.
All security controls must be tested to ensure they cannot be circumvented.	Devise and perform a test regime and retain the test results for at least two years.	Unidentified vulnerabilities in security controls could be exploited in the live environment. The level of risk is relevant to the purpose of the system/ network.
Network Prefix and published "bogon" filtering must be applied to the Internet network ingress and egress routing nodes.	Access controls lists should be defined for ingress and egress routing nodes. https://en.wikipedia.org/wiki/Bogon_filtering	Without this control invalid routing information could be propagated.
Whitelisting / Blacklisting - System interfaces or components must not accept unauthorised connections.	Criteria must be defined for allowing changes to the black/white list Alterations to any whitelist or blacklist should only be made under a changed controlled environment.	Access to destinations outside of any defined whitelist / blacklist may allow for users to access inappropriate sites and/or install software that has not been approved for use within your

Access should only be permitted that is required for correct network operation and for users to perform their day-to-day duties.	Reachability testing should be carried out to confirm the effectiveness of any white or black listing controls. Although not network management specific, this control can be backed up by implementing a company policy on the use of internet, email, and messaging; which could include conditions such as: "*Personnel must not bypass or tunnel through firewall or other security mechanisms*;" And *"Personnel must not install software that is not approved for use within the company*"	company. This may introduce vulnerabilities that could affect the confidentiality, integrity or availability of your service(s).
Access Control Lists (ACL) should be as detailed as possible.	The use of large source/destination subnets and wildcard masks should be avoided wherever possible.	Incorrectly configured access controls could allow access to wider the network area giving more opportunity to an attacker.
Disable dynamic routing on firewalls.	Vendor specific settings will need to be applied to ensure dynamic routing is not enabled.	Access control policy enforcement points may be bypassed.
Denial of Service (DoS), and Distributed Denial of Service (DDoS) protection.	Systems must be configured to protect services from DoS or DDoS attacks. This being from either the data, control or management planes.	The availability of service may be affected if a denial of service attack is experienced. Other attack vectors may be masked whilst such an attack is occurring.

2.4 Roles & Responsibilities

Recommended Control	Mechanism	Reason For Control
Ensure personnel complete appropriate technical training for the products they support.	The switch/router installation and support teams should be trained to a standard either tailored to the specific vendors equipment or an industry recognised, technical standard e.g. Cisco CCNA, Nortel NNCFS, etc. Additionally, the support staff must operate within the security policy of the network they are protecting.	Lack of appropriate training may lead to Switches/routers being delivered and controlled in an insecure manner which could allow unauthorised access, modification or unavailability.

2.5 Physical Security

Recommended Control	Mechanism	Reason For Control
Protect any removable media (such as flash drives).	Increasingly switches and routers are being supplied with embedded or removable flash memory drives for storing configuration and log files. These must be physically secured so as to prevent them from being easily removed, such as being protected by at least a locked door to the switch or router. It is suggested that an alert is generated upon the removal or insertion of such media.	Failure to secure removable media may lead to Information leakage - configuration and log files could help an attacker better compromise the device.

2.6 Failure Protection

Control	Mechanism	Reason For Control
Maintain hardware and software according to manufacturers' specifications.	All patches and upgrades relevant to the deployment should be tested on a non-live platform before the patch/upgrade is released in to a live environment. Any exceptions to this must have Domain owner approval. Patches should be applied according to their criticality and potential for exploitation in context of the deployment. Any patches/upgrades which are not applied must be documented and have Domain owner approval. Hardware maintenance should be covered by support agreements with the switch/router vendor.	To prevent failures in hardware due to poor maintenance.
Capacity Management processes.	Capacity requirements may be defined/determined from modelling the network, stress testing within test environments, or from planned requirements specified in the network design.	To prevent degradation of service due to exhausted capacity.
Have business continuity plans for critical networks.	Business continuity plans must be defined, implemented, exercised and reviewed. A critical network is one where the loss or unavailability of it could result in penalties, loss of market share or customer confidence.	To prevent failure or prolonged service disruptions caused by lack of business continuity measures.
Backup and Recovery	A back-up and recovery strategy should be defined, implemented and tested.	To prevent failure or prolonged service disruptions caused by lack of business continuity measures.

	For example securely storing of network device configurations, to allow rollbacks should any change adversely affect a network.	

2.7 Access Control

Recommended Control	Mechanism	Reason For Control
User access and authorisation processes must be implemented to secure the network and network devices	• Ensure all users' access has been authorised by persons who are responsible for the data or system. • Ensure all authorisations have been verified using a documented process. Utilisation of an authentication, authorization and accounting (AAA) solution, such as RADIUS or TACACS+ is recommended.	To prevent unauthorised access to and on the switch/router.
Keep roles of business use segregated. Segregation between system operations, developers, engineers, and network management must be maintained.	Using an AAA monitoring solution, the segregation must be enforced at least at the userid level i.e. the same userid cannot share the different group functions.	To prevent unauthorised access to and on the switch/router.

The network must implement a user id allocation and management process.	• Ensure all user ids are unique to an individual user. • Ensure closed/deleted user ids are not re-used. • Ensure that the allocation of temporary user ids, e.g. training user ids, is to a named individual and is recorded with the date, time and purpose. The use of remote AAA monitoring solution (RADIUS or TACACS+) is recommended.	To prevent unauthorised access or access attempts by a user account not being accountable to a person.
Your passwords, PINs, tokens, and conferencing access are for your eyes only, except when you're dealing with technical support. You must store them securely and separately from the device they're used to access. If you think someone has learned your password, change it immediately.	When using remote AAA services shared local user accounts must be created in case of loss of communication with the AAA server. These accounts must be able to manage the switch/router and must be controlled in number. Use of these accounts must be strictly controlled preferably by a central administration group.	To prevent unauthorised access or access attempts to lower level information by a user account not being accountable to a person.
User ids must be at least 6 characters long.	The use of an employee identification number, or email address is acceptable as a user id. This part of the standard must be enforced at the switch/router level and at a policy level administrators must be informed as to how to create a secure user account. The use of an AAA solution can enforce this part of the standard.	To prevent easily guessable user account names.

Trained Personnel	You must make sure that your people are appropriately trained before they use/access network devices or network management applications.	To ensure that access is restricted to only those users who are currently authorised.
The network must implement a user access review process.	Ensure that user accounts are reviewed in conjunctions with users' line managers to confirm they are still required.	To prevent redundant userids remaining enabled on the system. If an attacker could guess the password then they could access the system without being noticed.
When staff leave your organisation you must recover all assets and information, and remove all access.	Creation of a leaver's checklist can aid in this procedure.	To ensure that access is restricted to only those users who are currently authorised.
During the log-on sequence users must be required to acknowledge their obligations under relevant legislation, such as the Computer Misuse Act (in the UK).	This part of the standard should be enforced at the switch/router level.	If the Computer Misuse Act warning screen is not in place and the user does not have to positively confirm their access then it may prove difficult to prosecute unlawful access.

Network devices must not be deployed with default credentials.	Any default or supplied user ids or passwords e.g. manufacturers' supplied passwords, must be changed as soon as the device is enabled within a company environment. For wireless environments, change wireless vendor defaults, including but not limited to, removal of wired equivalent policy (WEP) keys, default service set identifier (SSID), passwords and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication. This should include default user accounts (including an enable passwords), control plane authentication keys (e.g. MD5 keys for BGP) and management protocol keys and passwords (e.g. SNMP v1/2c community strings, v3 usernames/passwords and authentication/encryption keys).	To prevent an attacker using a publicly known default password to gain unauthorised access to a switch/router.
The allocation of user passwords must be controlled through a formal management process.	Passwords must be distributed separately from the associated userid.	To prevent an attacker intercepting a user's password.
Passwords must be treated as sensitive information assets.	As a minimum, passwords must be treated as 'In Confidence' but where a password gives access to information at a higher classification the password may need additional controls to protect it.	To prevent an attacker intercepting a user's password.

Passwords must not be easily guessable and not be discoverable using dictionaries of commonly used passwords.	Password strength must be enforced by the system and be: • As random as possible • Not related to the userid, users identity or date • At least 8 characters long • Contain at least one character from (!,£,", $, %,^, &,*, (,), -,_, +, =, :, ;, ', @, ~, #, ?, <, >,) • At least one decimal number: (0... 9) • At least one capital case letter: (A... Z)	Without strong passwords user accounts can be exploited for unauthorised access.
Passwords must be periodically changed according to the classification of the information being accessed.	Passwords must not be reused within a 12 month period.	If passwords are used for long periods of time they may become more easily guessable and user accounts can then be exploited for unauthorised access.
Passwords must be reset through a formal management process.	• Passwords must only be reset if the identity of the individual is verified. • Reset passwords and initial passwords must be unique and the system must force a change on first use.	Without adequate verification user accounts can be exploited for unauthorised access.

2.8 Cryptographic Keys

If there are any requirements to encrypt content, the following controls are recommended:

Recommended Control	Mechanism	Reason For Control
Cryptographic key generation	All keys should be generated using a secure random number generator (e.g. Solaris /dev/random) and include at least 6 bits of entropy per character. To obtain full security keys meeting the previous requirement should be at least 22 characters in length (giving more than 128 bits of entropy). Keys should not be less than 16 characters in length (giving 96 bits of entropy).	To prevent insecure keys generated.
Cryptographic keys must meet or exceed a minimum length.	Symmetric keys (e.g. AES) must have a key length of at least 128 bits. Asymmetric keys (e.g. RSA) must have a key length of at least 2048 bits.	Shorter key lengths can be easily compromised within the lifetime of the data.
Use only known and trusted cryptographic ciphers.	Use industry best practice secure coding standards.	Untried and tested ciphers introduce unknown vulnerabilities.
Private keys must be protected to a level commensurate with the classification of the data they are associated with.	Implement logging and alarming of private key operations, and investigate alarms or log anomalies, e.g. unexpected accesses. Use a passphrase containing more than 12 mixed alpha-numeric characters and symbols. If the passphrase must be written down it must be placed in an envelope and stored in a safe with access limited for approved personnel only.	If a private key is compromised it could result in the entire system being compromised.

If it is possible to gain shell level access to the switch or router it must be documented and all access to the shell must be strictly controlled via strong authentication, authorisation and all activity must be logged.	The use of an AAA protocol with strong authorisation and accounting functionality and a specific user account role to restrict access is recommended.	To ensure that access is restricted to only those users who are currently authorised and prevent unauthorised elevation of privilege.

2.9 Auditing

Recommended Control	Mechanism	Reason For Control
Monitoring of event logs must be performed.	Security monitoring procedures must be implemented which ensure that audit data is inspected using appropriate tools and techniques. The procedures will include: • Who is responsible for inspecting the audit data • Which events must be monitored • How events will be monitored • The frequency of monitoring • What to do when suspicious activity is noted • When to escalate and via what mechanism Action must be taken to rectify the situation when the security audit trail or log files become unavailable for any reason and the system continues to operate. An alarm should also be triggered when this situation occurs. All alarm types must be documented for operational management.	If audit logs are not analysed then security events or trends may continue.
The audit logs must be removed from the switch/router and transported to a central management server.	This can be achieved through the use of Syslog or a secure file transfer protocols such as SFTP or SCP.	To prevent records of any unauthorised access and/or modification to the switch/router not being available for accountability, evidential or investigative purposes.

2.10 Development & Support

Recommended Control	Mechanism	Reason For Control
Incident and problem management.	Processes should be designed and implemented to handle network incidents, and problems. This process should tie into the change control process mentioned previously.	Problems being poorly managed may result in extended service outages, data loss and vulnerabilities not being properly resolved.
Segregation of Environments	Keep production and non-production environments segregated.	To prevent unauthorised access or modifications to systems in a production environment caused by poor segregation between environments.
Acceptance into Service	A process should be defined to ensure new network features are thoroughly tested before they are accepted into service.	To minimise the risk of switch/router failures following upgrades or new software implementations.
Operating procedures must be unambiguous, contain all of the instructions required to operate the system and include the steps to be taken in the event of failure or unexpected behaviour of the system.	The following areas should be considered for inclusion in the procedures: • Access control • Start-up/Shutdown, • Clock Synchronisation, Application and Job Management, • Data Transfers, • Monitoring and Alarms, Problem and Escalation Management, • Back-up & Recovery, • Archiving, Migration, • Change Control, • Disaster Recovery / Fallback, • Hardware & Software maintenance, and application of security patches.	A lack of operating procedures could result in a system in an insecure state.

2.11 Document Control

Author	BT Security, 3rd Party Security Team
Owner & Approver	BT Security, 3rd Party Security Team

Document Review

Draft A – 19 April 16	Review comments BT Security, 3rd Party Security Team
Draft B – 20 April 16	Review comments BT Security, Policy team; BT Security, Network Assurance
Draft C – 26 April 16	Final Review comments BT Security, Policy team; BT Security, Network Assurance and BT Security, 3rd Party Security Team.
Issue 1.0 - 28 April 16	First issue following review

End of document