20.3. Virtual Local Area Networks

Objective

20.3.1. Virtual local area networks (VLANs) are deployed in a secure manner that does not compromise the security of information and systems.

Context

Scope

20.3.2. This section covers information relating to the use of VLANs within agency networks.

Multiprotocol Label Switching

20.3.3. For the purposes of this section Multiprotocol Label Switching (MPLS) is considered to be equivalent to VLANs and is subject to the same controls.

Exceptions for connectivity

20.3.4. A single network, managed in accordance with a single SecPlan, for which some functional separation is needed for administrative or similar reasons, can use VLANs to achieve that functional separation.

20.3.5. VLANs can also be used to separate VTC and IPT traffic from data traffic at the same classification (See Section 18.3 – Video and Telephony Conferencing and Internet Protocol Telephony).

Software Defined Networking (SDN)

20.3.6. Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and managed by a separate application described as a controller. SDNs are intended to provide flexibility by enabling network engineers and administrators to respond to rapidly changing business requirements.

20.3.7. Separation and Segregation principles also apply to SDNs. Refer to Section 22.2 – Virtualisation.

References

20.3.8. Further references can be found at:

Reference	Title	Publisher	Source
IEEE 802.1Q-2011	**IEEE Standard for Local and Metropolitan area networks – Media Access Control (MAC) Bridges, and Virtual Bridged Local Area Networks.**	Institute of Electrical and Electronics Engineers (IEEE)	IEEE SA - The IEEE Standards Association - Home
	Inter-Switch Link and IEEE 802.1Q Frame Format	CISCO	Inter-Switch Link and IEEE 802.1Q Frame Format - Cisco
	Dynamic Trunking Protocol (DTP)	CISCO	Virtual LANs VLAN Trunking Protocol (VLANs VTP) - Cisco

Rationale & Controls

Using VLANs

20.3.9.R.01. **Rationale**

Limiting the sharing of a common (physical or virtual) switch between VLANs of differing classifications reduces the chance of data leaks that could occur due to VLAN vulnerabilities. Furthermore, disabling trunking on physical switches that carry VLANs of differing security domains will reduce the risk of data leakage across the VLANs. The principles of separation and segregation must be applied to all network designs and architectures.

20.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4942]

The principles of separation and segregation MUST be applied to the design and architecture of VLANs.

20.3.9.C.02. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:4943]

Agencies MUST NOT use VLANs between classified networks and any other network of a lower classification.

20.3.9.C.03. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4944]

Agencies MUST NOT use VLANs between any classified network and any unclassified network.

20.3.9.C.04. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4945]

VLAN trunking MUST NOT be used on switches managing VLANs of differing security domains.

Configuration and administration

20.3.10.R.01. **Rationale**

When administrative access is limited to originating from the highest classified network on a switch, the security risk of a data spill is reduced.

20.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4948]

Administrative access MUST be permitted only from the most trusted network.

Disabling unused ports

20.3.11.R.01. **Rationale**

Disabling unused ports on a switch will reduce the opportunity for direct or indirect attacks on systems.

20.3.11.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4951]

Unused ports on the switches MUST be disabled.

20.3.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4952]

Unused ports on the switches SHOULD be disabled.