NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

This is a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide. It is developed exclusively by the ERO Enterprise under its obligations for independence and objectivity. This CMEP Practice Guide is intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities. This CMEP Practice Guide is posted publicly solely to provide transparency.

ERO Enterprise CMEP Practice Guide:

Assessment of Virtualized Storage
February 26, 2021

Background

In support of successful implementation of and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.

Purpose

This CMEP Practice Guide provides guidance to ERO Enterprise CMEP staff (CMEP staff) when assessing a Responsible Entity's Cyber Assets that provide access to storage via technologies such as Network Attached Storage (NAS), Network-Tunneled Storage (e.g., iSCSI), and Storage Area Networks (SAN). This Practice Guide outlines risks that CMEP staff should consider when verifying methods used to meet the security objectives. This risk information informs CMEP staff's understanding of a Responsible Entity's security posture and commensurate Compliance Oversight (i.e., Compliance Oversight Plan, audit approach, etc.). CMEP staff make compliance determinations in light of the specific facts and circumstances of the individual registered entities and the language of the Requirements.

General Approach

CMEP staff should consider Cyber Assets providing functions for Cyber Assets within an Electronic Security Perimeter (ESP) and Cyber Assets outside an ESP to be shared infrastructure. CMEP staff should verify that the Responsible Entity identifies and protects any Cyber Asset providing shared infrastructure, regardless of type, to the "highest water mark" of CIP compliance. In other words, each Cyber Asset providing shared infrastructure must comply with the applicable CIP Requirements for all BES Cyber Systems to which it connects. If a Cyber Asset providing storage meets the definition of Physical Access Control Systems (PACS) or Electronic Access and Control or Monitoring Systems (EACMS), CMEP staff would assess the storage essential to the PACS or EACMS service against the Requirements applicable to a PACS or an EACMS, respectively.

Virtual Storage

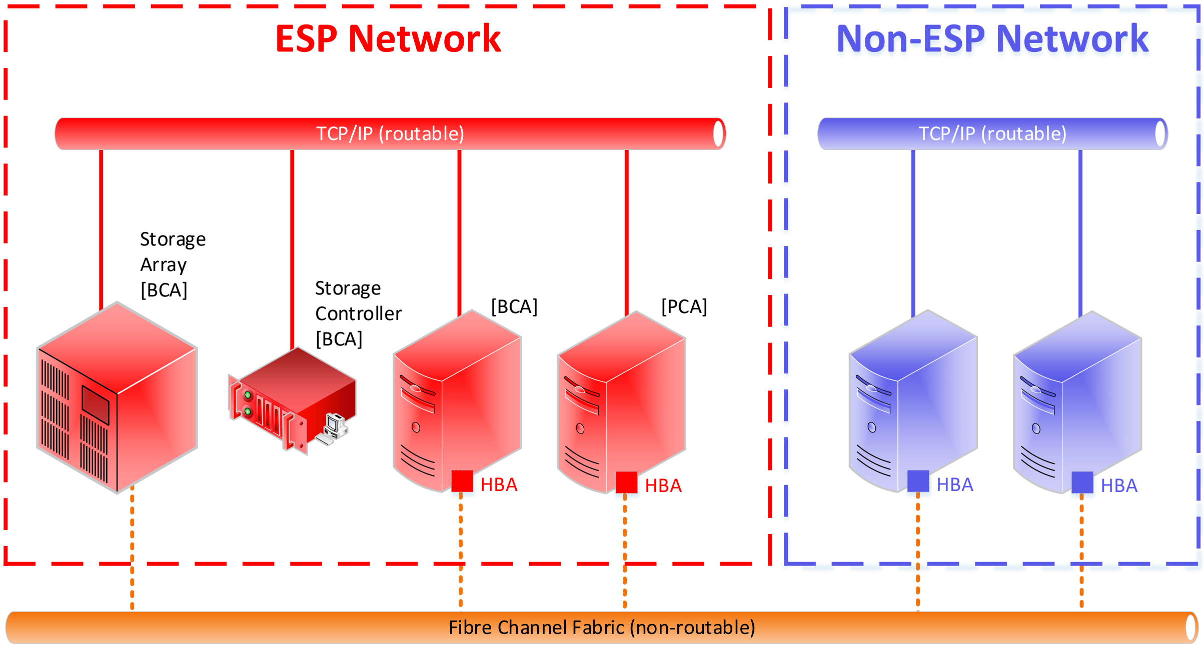
NAS devices share disk space according to common client-server technologies. A NAS device functions much like a network server with a large amount of locally-attached storage.

[1] The ERO Enterprise consists of NERC and the Regional Entities
[2] The ERO Enterprise Compliance Guidance Policy

iSCSI storage arrays (or "network-tunneled" storage technology) attach a large array of storage to an appliance that tunnels interface protocols, such as Small Computer Systems Interconnect (SCSI), across an Internet Protocol (IP) network. Network-tunneled storage devices appear as a special case of NAS. This technology functions much like network-tunneled remote serial ports. An endpoint needs a special software driver to attach a Logical Unit Number (LUN) or virtual disk. The operating system of the endpoint uses the iSCSI disk like it attached locally.

SAN configurations make large storage arrays available to Cyber Assets, generally through Fibre Channel (FC) connections, from the SAN controller to a Host Bus Adapter (HBA) installed physically in the server. SAN hardware provides failover, flexible storage, disk redundancy, and snap backups to attached systems. SAN disks truly "attach locally" in that the server may access files, "boot-to-SAN," and format virtual disks. Operating systems do not allow multiple servers to share a single LUN at the hardware level. With additional FC switches to create a FC fabric, multiple SAN configurations may interoperate to provide redundancy against data loss and downtime. Additional information can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-125: Guide to Security for Full Virtualization Technologies.[3]

Storage Area Network



In the example illustrated above, the SAN infrastructure is in a high or medium impact environment. In this example, the SAN is presumed to have a 15-minute impact on operations and has been identified and protected as a BES Cyber Asset (BCA). The SAN and its management controller reside within an ESP. Therefore, CMEP staff should assess controls down to the LUNs on the SAN, verifying that all controls comply with the highest security level and CIP Requirements of any applicable Cyber Asset connected.

[3] http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

Network Attached Storage

CMEP staff should assess NAS systems as traditional server-based, network drive shares, and assess compliance against the applicable CIP Requirements. If NAS traffic crosses the boundary of the ESP, the CMEP staff should verify that all External Routable Connectivity (ERC) traverses only through an identified EAP and in compliance with CIP-005 Requirements.

Network-Tunneled Storage

Network-tunneled storage systems, such as iSCSI, essentially share network drives across an IP network. Therefore, if the network-tunneled storage device resides within the ESP and does not communicate externally, CMEP staff should assess compliance against CIP-007 Requirements. If the network-tunneled storage device and its connected endpoints reside on opposite sides of the ESP boundary from one another, CMEP staff must verify that all ERC traverses only through an identified EAP and complies with CIP-005 Requirements.

If network-tunneled storage clients reside within the ESP, CMEP staff must verify the inclusion of any software installed for storage connection in the Responsible Entity’s CIP-007 security patch management and CIP-010 configuration change management programs.

Storage Management Devices

CMEP staff should verify that the management interface of any storage server, whether as a hardware component of a BES Cyber System, or as a stand-alone BCA/PCA, resides only within a defined ESP. Connections to the storage management interface, regardless of type, must comply with all applicable CIP Requirements.

CMEP staff should verify that the Responsible Entity controls electronic access to the management interface of the Cyber Asset providing shared infrastructure storage. Any electronic access to the management interface from sources external to the ESP should comply with Interactive Remote Access (IRA) Requirements and traverse the ESP boundary at an identified EAP, and meet compliance with applicable CIP-005 Requirements.

Low Impact BES Cyber System Considerations

In a low impact environment, any storage system should be evaluated for potential low impact BES Cyber System applicability. If so identified, physical and electronic access to the BES asset containing the storage system and its management components should be controlled in accordance with Attachment 1 of CIP-003.

Conclusion

In assessing a Responsible Entity’s CIP-applicable storage systems, CMEP staff should assess according to the high-water mark of any associated BCA, BES Cyber System, EACMS, PACS, or PCA. The management interface of a SAN controller provides electronic access to all Cyber Assets attached via FC. However, the management interface of a NAS (or network-tunneled system) provides electronic access only to the storage system itself. As in all other cases, any ERC must traverse an ESP boundary at an EAP. Storage system architectures differ, but when those architectures are consistently defined, common auditing practices apply to all.