

INTRODUCTION OF A NETWORK ACCESS CONTROL SYSTEM & STRATEGY FOR THE DEPLOYMENT THROUGHOUT PUBLIC HEALTH WALES (PHW)



Christopher Pace

1708232@student.uwtsd.ac.uk

Abstract

Network Access Control (NAC) is an approach to computer security that attempts to merge endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

Although PHW have a robust security architecture in place at present, it was decided that this needed to be improved to keep abreast of the current security threats being exploited in the wild.

After consultation with numerous Security Consultants to discuss the current security risks identified within PHW, it was suggested that the introduction of a Network Access Control (NAC) solution could help to eradicate the issues identified during the security review.

After a robust analysis of the current NAC solutions available on the market, it was decided that the best suited solution based on funding and feature set, that a Cisco ISE solution was to be implemented.

The aim of the project is to construct a Low Level Design (LLD) on how to implement a Cisco ISE solution within PHW.

What is Network Access Control (NAC)?

The main objective of NAC is to extend the security of networks to the end-point by evaluating the authenticity, integrity and security posture of each end-point prior to permitting network access.

Today's NAC is changing beyond the "traditional" Authentication, Authorization, and Accounting (AAA) into dynamic solutions with improved integrations that discover, monitor, and enforce policies expanding past enterprise walls. NAC is a foundational network security defence as every device on a network is a potential attack or reconnaissance point that must be discovered and secured.

To do this, the following functional areas must be present: authentication/authorization, assessment of security posture, quarantine and remediation.

Cisco ISE offers all of the above functions as well as others (see **Cisco ISE Features** below).

Aims & Objectives

The aim of the project is to construct a LLD and Proof of Concept (POC) on how to implement a Cisco ISE solution within PHW Due to time constraints and complexity of implementation only focusing on deploying the following NAC features:

- Access Control
- Asset Visibility
- Device Admin
- Threat Control

Methodology

A thorough review of the current Cisco ISE documentation will be completed, as well as attendance on the Cisco ISE Implementing and Configuring Cisco Identity Services Engine (SISE) Instructor-led course. After completion of the review/course a LLD will be collated focusing on a single PHW Site. On completion of the LLD a POC will be implemented within the chosen PHW Site in monitoring mode only in order to not affect live services running out the chosen site.

	Asset Visibility	Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.
	Access Control	Consistent access control across wired, wireless and VPN Networks. 802.1X, MAC, Web Authentication and Easy connect for admission control.
	Guest Access	Fully customizable branded mobile and desktop guest portals, with dynamic visual workflows to easily manage guest user experience.
	BYOD Access	Simplified BYOD management with built-in CA and 3rd party MDM integration for on boarding and self-service of personal mobile devices

	Segmentation	Topology Independent Software-defined segmentation policy to contain network threats.
	Context Exchange	Context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.
	Threat Control	Protection against threats across the attack continuum, before, during and after an attack. Reduce time-to-detection from days to hours.
	Device Admin	Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices