Feasibility Study NAC for Vanderlande Industries

Stefan Roelofs
stefan.roelofs@os3.nl

February 1, 2009

UNIVERSITEIT VAN AMSTERDAM

Supervisor:
ir. Marcel Verbruggen

Abstract

This report covers a feasibility study for the introduction of Network Access Control (NAC) at Vanderlande Industries. The focus of this report is on a network based access control architecture with as main research questions:

What is the best architecture for a NAC solution in this environment?
To answer this question, the different stages of network based NAC and their possible techniques are discussed. In chronological order these stages are: detection, registration and authentication, policy enforcement, pre-admission control, access classification and post admission scanning. In the chapters about these stages, practical issues to implement them at the company will be unfolded. Also, a number of sections contain practical verifications of the findings.

What elements and services should be part of this architecture?
Elements and services that should be part of the architecture are placed in different environments the NAC solution can place clients into. In these environments, services as authentication, remediation (e.g. update repositories) and health check systems (e.g. vulnerability scanners and intrusion detection systems) need to be deployed.

What organizational processes should be in place for an introduction of this technique?
The architecture unfolded in this report is mainly based on the self-service aspect of the future users. Because of this, only IT management and helpdesk support processes should be in place. Next to this, the current processes on adding extra network equipment, asset management and the hardening of clients should be reviewed.

Is network based NAC feasible technology for this situation?
Some specific elements from a client-based approach are needed to make the solution complete. In general, the network based approach fits the company situation.

Acknowledgements

I would like to offer gratitude to the following people and organizations:

- Vanderlande Industries for providing the means and opportunity to conduct this research project.
- Marcel Verbruggen, my supervisor, for offering help, support and ideas.
- All those who gave their feedback on this document.

Contents

1 Introduction **7**
1.1 Background . . . 7
1.2 Research Questions . . . 7
1.3 Scope . . . 7
1.4 Approach . . . 8
1.5 End result . . . 9

2 Company introduction **10**
2.1 Vanderlande Industries . . . 10
2.2 Locations . . . 10
2.3 Users . . . 11
2.4 Technical Situation . . . 11
2.4.1 Network infrastructure . . . 11
2.4.2 Critical network services . . . 12
2.4.3 Endpoints characteristics & security . . . 12
2.4.4 IP Addressing & Assignment . . . 13
2.4.5 Network security . . . 13

3 Introduction to Network Access Control **14**
3.1 Goals . . . 14
3.2 Terminology . . . 14
3.3 Agent versus agent less concepts . . . 15
3.4 Capabilities . . . 15

4 Element detection **17**
4.1 802.1x . . . 17
4.2 Simple Network Management Protocol (SNMP) . . . 17
4.2.1 Startup sequence . . . 17
4.2.2 Shutdown sequence . . . 18
4.3 Mapping of MAC - IP addresses . . . 18
4.4 VI Case . . . 19
4.4.1 802.1x versus SNMP detection . . . 19
4.4.2 Mapping of MAC - IP addresses . . . 19
4.4.3 Practical verifications . . . 20

5 Registration & authentication **24**
5.1 Registration . . . 24
5.1.1 Repository . . . 24
5.1.2 Central based approach . . . 24
5.1.3 User based approach . . . 24
5.2 Authentication . . . 24
5.2.1 Registration is authentication . . . 24

5.2.2 802.1x . . . 25
5.2.3 Captive Portal & Registration VLAN . . . 25
5.3 VI Case . . . 26
5.3.1 Registration . . . 26
5.3.2 802.1x and captive portal VLAN . . . 26
5.3.3 Guest Users . . . 27
5.3.4 Static IP clients & no browser clients . . . 27
5.3.5 Extra network equipment . . . 28
5.3.6 Administrative access . . . 28

6 Policy enforcement **29**
6.1 802.1x . . . 29
6.2 ARP . . . 29
6.3 In-line devices . . . 30
6.4 DHCP . . . 30
6.5 Dynamic VLAN . . . 31
6.6 Administrative access . . . 31
6.7 VI Case . . . 31
6.7.1 Policy enforcement . . . 31
6.7.2 Assign random VLAN numbers . . . 32
6.7.3 Private VLAN . . . 32
6.7.4 Administrative access . . . 33
6.7.5 Practical verifications . . . 33

7 Pre-admission evaluation **35**
7.1 Vulnerability scanning . . . 35
7.2 Intrusion detection . . . 35
7.3 User interaction . . . 35
7.4 VI-Case . . . 36
7.4.1 Vulnerability scanning . . . 36
7.4.2 Intrusion detection . . . 37
7.4.3 User Interaction . . . 37
7.4.4 Known MAC allowance . . . 38
7.4.5 Pre-register MAC . . . 38
7.4.6 Practical Verifications . . . 38

8 Access classification **40**
8.1 Authentication & remediation environment . . . 40
8.2 Guest environment . . . 42
8.3 Production environment . . . 43
8.4 Wrap up . . . 43

9 Post-admission scanning **44**
9.1 Guest environment 44
9.2 Production environment 44
9.2.1 Vulnerability scanning 44
9.2.2 Intrusion Detection 45

10 Organizational processes **46**
10.1 Registration & Authentication 46
10.1.1 Registration limits 46
10.1.2 Pre-registration 46
10.1.3 Authentication 46
10.1.4 Extra network equipment 46
10.2 Asset management 47
10.3 Management effort 47
10.4 Hardening clients 48

11 Conclusion & future research **49**
11.1 Final thoughts 50
11.2 Future research 50

Appendix A Endpoint Security Threats **57**

Appendix B 802.1x Flowchart **58**

Appendix C Captive Portal Flowchart **59**

Appendix D Snort Rules **60**

Appendix E Environments Overview **62**

List of Figures

1 SNMP Host Detection Startup 18
2 SNMP Host Detection Shutdown 18
3 Captive Portal 25
4 ARP influencing 29
5 Private VLAN 32

1 Introduction

This report covers the feasibility of a possible introduction of Network Access Control (NAC) at Vanderlande Industries (VI). In the light of recent progress on network based NAC solutions, VI would like to see if this is a feasible architecture to introduce NAC on their internal network.

1.1 Background

VI is a global player in the market of material handling products. Because of its worldwide presence and solely project based approach it requires a highly flexible IT environment. The IT network infrastructure hosts many different types of systems (e.g. industrial systems) and people (e.g. subcontractors). VI expects that a NAC solution will bring:

- Regulation as to whom has access to the internal IT network and by what means.
- Protection of systems against infections from viruses, malicious software and OS exploits.
- Protection against malicious network activities such as rogue DHCP servers, port scans and rogue mail servers.
- Protection of company data and users by enforcing a basic set of security measures on every corporate host.

1.2 Research Questions

This report will provide an answer to the following research questions:

- What is the best architecture for a NAC solution in this environment?
- What elements and services should be part of this architecture?
- What organizational processes should be in place for an introduction of this technique?
- Is network based NAC feasible technology for this situation?

1.3 Scope

The project will have the following scope:

- The research will concentrate on the Vanderlande Industries network located in Veghel (The Netherlands). The architecture of branch offices and project locations will be described in a general way.

- The investigation will not cover the wireless network of Vanderlande Industries.
- Implementation concerns with current server hardware and/or software compatibility, contracts or commercial decisions will not be part of the research.
- Thorough investigation of the effect on current Voice over IP services (VoIP) and Quality of Service (QoS) will not be part of the research.
- Supervisory Control And Data Acquisition (SCADA) internal communication networks (Profibus, Profinet) will not be part of the research. Only SCADA hardware and operating systems directly connected to the main network will be investigated.

1.4 Approach

1. Have questionnaire with IT, IT security and industrial engineering staff concerning regulations and demands on solution.
2. Map company environment and employee characteristics.
3. Map current network and services.
4. Globally map current endpoint security threats (a thorough analysis on this will not be part of the research since this would require too much resources)
5. Investigation of possible architectures with special focus on network based NAC:
   (a) Investigate if the architecture secures against earlier mapped endpoint security threats.
   (b) Deployment of components in the network for optimum results.
   (c) Investigate if the architecture suffices regulation requirements.
6. Investigate organizational processes concerning chosen architecture.
7. Build test environment/components with network based NAC solution (open-source implementation PacketFence)
8. Conduct tests to verify architectural findings.
9. Write final advisory report.

1.5 End result

The end result of this feasibility study is the report you are now reading. This report should provide VI a view on a NAC architecture for its organization and what impact this will have on its current technical and organizational situation. This report will first provide a description of the company, its different IT users and technical infrastructure. An introduction to NAC and its general terminology will follow. Next, the different NAC stages will be outlined in chapters 4 to 9. These chapters will start with a general description of the stage, followed by the VI case. In chapter 10, organizational processes surrounding a possible introduction of NAC will be discussed. Finally, in chapter 11 conclusions will be presented. During the research, components were tested to verify findings. The results of these tests (if present) will be outlined per chapter.
With this report it should be possible for VI to start an implementation phase, in which large scale proof of concepts can be conducted to verify compliance on the architecture presented in this report. The goal of this report is therefore not to describe the ideal situation but a practical view on current techniques and its possibilities.

2 Company introduction

Before discussing the main subject it is necessary to provide a view on the company this feasibility study is carried out for and outline its current technical situation.

2.1 Vanderlande Industries

Vanderlande Industries (VI), founded in 1949 in Veghel near Eindhoven (The Netherlands), has a long history in the material handling market. Currently the company provides automated electrical systems in the following three main markets [1]:

- Baggage handling (i.e. airports)
- Express parcel (i.e. sorting hubs)
- Distribution (i.e. warehouses)

The company currently employs around 1742 FTE [2] worldwide, of which approximately 1000 are based at its headquarters in Veghel. 50% of the employees have a college or university degree.

> "The company and its employees can be typed as highly innovative and flexible to provide the needs of its customers."[1]

The company follows a project based approach where projects can last one month to several years, depending on the size of the ordered system. Next to this, VI delivers service on material handling systems for its customers. The IT department of VI is solely internal based and contains two sub departments that are of interest to this study: IT infrastructure (system/network administration) and IT infra/projects (system/network engineering for (internal) company and customer projects)

2.2 Locations

VI's presence can be categorized in the following types:

- Office locations (permanent)
- Project locations (temporary depending on the size of the project)
- Service locations (long-term temporary depending on the contract time)

Most VI locations lack a strict guest administration and/or physical access control. Only server rooms are considered physical secure and are accessible by a limited group of IT management personnel.

2.3 Users

Since this report focuses on whom must have access to IT facilities and by what means, it is necessary to classify these (possible) users.

- Employees in service of the company (long-term).
- External employees and interns with a mid-term presence.
- Mid-term guests such as subcontractors or partners on a specific project.
- Short-term guests whom mostly take care of a specific task.

2.4 Technical Situation

In order to outline an advisory on the placement of a NAC solution in the infrastructure, it is essential to map the current situation.

2.4.1 Network infrastructure

When VI's LAN network is mapped against Cisco's three tier model [3] it can be determined that the network follows a "collapsed core" design where there is no distribution layer. All distribution layer functionality is done by the core. The core layer performs OSI layer 3 "switching". Access layer devices are OSI layer 2 devices. Static VLAN's are defined at the core switches primarily for WLAN's and Voice over IP (VoIP).
The WAN design makes use of MPLS and IPsec VPN tunnels over the Internet to build connections to office, project and service locations. These connections are built up as a logical star, making the headquarters in Veghel the center of the star. Supervisory Control And Data Acquisition (SCADA) systems are built around industrial switches which run Profinet [4]. This field bus Ethernet standard uses three different types of protocols:

- TCP/IP for non real time communication with electric peripherals in the range of 100 ms;
- RT (Real-Time) for I/O communication up to 10 ms per cycle;
- IRT (I synchronous Real-Time) for I/O communication less than 2 ms per cycle.

Since these networks are left out of the scope of this project (see paragraph 1.3) it is only important to be aware of the fact that these networks may be situated beyond standard endpoints such as PLC equipment.

2.4.2 Critical network services

Critical network services are currently deployed around two servers on the headquarters of the location Veghel. These servers hold LDAP services, DNS and DHCP services. The two servers are a standby for one another. These services are critical for the following reasons:

- LDAP Services for authentication and authorization services
- DNS for internal and external name resolution
- DHCP services for IP assignment on all VLAN's.

These services are also deployed on project, service and office locations depending on the number of users and the availability of a physical secure location to host them.

2.4.3 Endpoints characteristics & security

Network endpoints are defined as network devices connected to IT network equipment of VI. These endpoints can demark internal or external administrative jurisdiction. The following hardware devices can be defined as endpoints:

- Workstation or server systems x86 based systems.
- SCADA equipment such as Programmable Logic Controller's (PLC's) and sensors telemetry.
- Network peripherals such as printers.

PLC's are programmed with Ladder logic [5], have no underlying operating system and use network expansion cards running a limited configurable vendor proprietary IPv4 stack. Other corporate operating systems comprise:

- Microsoft Windows
- QNX (Unix family OS with support for real-time protocols see paragraph 2.4.1)

Appendix A (page 57) outlines the different security threats these operating systems pose.
Although the company employs around 1750 FTE, network components are estimated well over 4000. This is mainly due to high number of engineers at VI, which may host a simple server to multiple servers or hardware equipment connected to the network. Every new workplace at VI is equipped with 3 network connection outlets.

2.4.4 IP Addressing & Assignment

VI uses RFC1918 [6] addresses and 2 other public /24 subnets for internal usage. RFC1918 address ranges are also used on customer projects. Some IP ranges are re-used when a project is soled. Also, some IP address ranges of customers may be used in test setups which are shipped to customer locations after design tests. IP address assignment is done through DHCP servers mostly for standard office equipment. Address assignment for industrial hardware is done through static IP assignment. The registration of these IP devices is maintained in an IP library. For external hosted networks (mostly connected by VPN) however, address assignment is by subnet and administration is done on initiative of the hardware engineer or project leader requesting the subnet. Sometimes this is administration is not done at all or isn't updated after an initial inventory. Registration of devices in the IP library is not consequently accompanied by the MAC address of the device. In this report there will be a separation in the type of address assignment to endpoints:

- DHCP Capable clients: endpoints with automatic IP configuration through DHCP with a user actively controlling them (i.e. office client equipment).
- Static clients: endpoints with static IP configuration, usually with no user actively controlling them (i.e. servers, printers and industrial automation equipment).

2.4.5 Network security

The current network security comprises antivirus products and perimeter network firewalling. Currently, McAfee antivirus is deployed on all standard office equipment. No client firewalling is active. On the perimeter network, where WAN and Internet connections are deployed, Cisco based IPS sensors are active.

3 Introduction to Network Access Control

> "..the definition of what NAC is, what components a NAC solution should (and/or must) have, and what does a NAC solution needs to adhere to varies from one vendor to another (..) Network Access Control (NAC) is a set of technologies and defined processes, which its aim is to control access to the network allowing only authorized and compliant devices to access and operate on a network"[7]

When looking at different implementations [9] on the Internet, this quoted view of Ofir Arkin [8] comes close to what is the general impression. However, there is a common framework, the Trusted Network Connect (TNC) promoted by the Trusted Computing Group (TCG).

> "The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices."[10]

The organization itself however is not supported by all NAC vendors. Also, some critics consider the group as a hazard for user privacy [11] Since these criticisms are mostly from the open-source community, developers of open-source NAC initiatives might not be motivated to make their implementations interoperable with TCG specification systems.

3.1 Goals

Goals to implement NAC may vary, but are usually built around one or both of the following principles:

- Protect IT resources, data and users against malicious hosts.
- Require a basic set of security measures on every connecting host also protecting the host from threats originating on it.

3.2 Terminology

The TCG introduces some common terminology to define NAC components:[12]

- Access Requestor (AR): the endpoint requesting access to the network.
- Policy Decision Point (PDP): the software which holds the company policies NAC must enforce and makes the decisions on the AR request.

- Policy Enforcement Point (PEP): the network equipment that enforces the PDP's decision.

Since this terminology universally fits different architectures it will be used throughout the rest of this report.

3.3 Agent versus agent less concepts

Most NAC systems are built around one of two concepts: agent or agentless (also called network based) NAC systems. These concepts are all focused on how to gain knowledge of the AR's health. In case of agent systems, the AR is equipped with a persistent agent who communicates with the PDP. In case there is no administrative jurisdiction over the AR a dissolvable agent by means of mobile code can be executed (e.g. Java or ActiveX components) [9]. Agent less systems are solely based on information retainable from network components or by means of Remote Procedure Call (RPC). Network components that can provide crucial AR information include vulnerability scans and passive network scans such as intrusion detection systems.
Persistent and dissolvable agent systems hold various downsides [9]. To install or run an agent, administrative rights on the AR are needed to check the condition of various elements. Next to that, most vendors only supply agents for common operating systems. For VI's situation this can be complicated because of numerous different (or non standard) operating systems connected to the network. Because of these reasons, this report will focus mainly on a network based NAC approach. Agentless systems [9] have the advantage that there are no modifications necessary to the AR. Next to the lower administrative burden of client software, this technique is also applicable to legacy and non-standard equipment. The focus of this report is mainly on network based NAC because of its non-intrusive approach and possible compatibility with VI's industrial automation equipment (2.4.3) connected to its network.

3.4 Capabilities

To enforce company policies to end systems, NAC solutions generally must have the following capabilities or stages: [7]

1. Perform element (AR) detection.
2. Register & authenticate the AR and/or user.
3. Perform a minimal set of necessary checks (pre-admission evaluation) on the health of the AR.
4. Provide a way to enforce policy on the AR and/or bound it to a certain environment.

5. Provide a broad set of continues checks (post-admission control) on the health of the AR.

The following chapters of this report are based on these stages.

4 Element detection

Element detection is the first crucial stage of a NAC solution.

> "Element detection must detect, in real time, a new element, as it attempts to attach itself to the network" "It is simply because you cannot expect a NAC solution to defend against devices it is not aware of".[7]

This section outlines different strategies to detect new elements on a network.

4.1 802.1x

802.1x [13] is an IEEE standard for port-based network access control. 802.1x works with a "supplicant" (AR) which needs to authenticate to an authentication server (PDP) such as RADIUS. The supplicant starts in an "unauthorized" mode in which the authenticator (PEP) blocks all traffic except 802.1x traffic. Next, the authenticator sends out an EAP-Request to the supplicant, as where the supplicant will answer with his/her credentials or certificate. The authenticator forwards these to the authentication server which makes the policy decision to configure the switch port to "authorized" enabling all network traffic. 802.1x requires all AR's and PEP's to have 802.1x capabilities, although it is possible to specify exceptions (usually by MAC address).

4.2 Simple Network Management Protocol (SNMP)

> "SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention"[14]

This section describes the model on how to use SNMP in a NAC situation. Discussion on differences and why choosing for a specific version of the SNMP protocol is beyond the scope of this report, but the interested reader is referred to [15]. In example figures 1 and 2 the AR is displayed as an ordinary workstation seeking network access but this could be any type of network device. Element detection by SNMP largely depends on the registration of the MAC address. With this unique hardware address it is possible to identify an element on the network. The MAC address however, is susceptible to spoofing [16], a security concern which should be addressed.

4.2.1 Startup sequence

Figure 1 displays the startup process that can be used to detect a new element through SNMP. In this figure, the PEP is configured to send linkUp

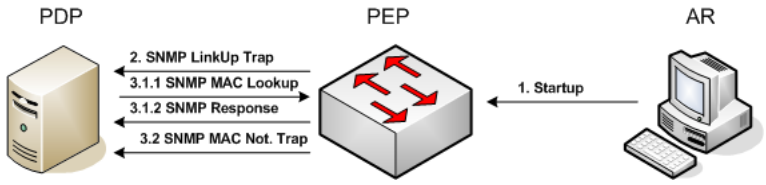


Figure 1: SNMP Host Detection Startup

and linkDown SNMP traps to the PDP. When an AR boots up (1), the PEP will send numerous linkUp and linkDown traps to the PDP (2) [17]. Since it will take some time for the PEP to detect the MAC address of the AR, the PDP will have to send numerous SNMP ”get” requests on the MAC address property of the specific port (3.1.1). When the MAC is known on the PEP, the MAC address will be send to the PDP (3.1.2) which is now able to register the node. Some switches also support the MAC Notification SNMP Trap (3.2) which makes the numerous SNMP polling from the PDP obsolete.

4.2.2 Shutdown sequence

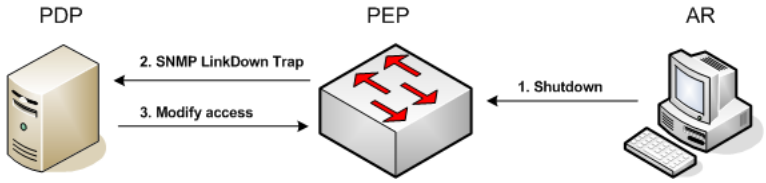


Figure 2: SNMP Host Detection Shutdown

Figure 2 displays the shutdown process that the SNMP process will follow. When the AR shuts down (1), the PEP sends a linkDown trap to the PDP (2) which enables it to disable or modify access of the switch port at the PDP (3).

4.3 Mapping of MAC - IP addresses

In order to let a NAC system use information from multiple sources dispersed throughout the network it is essential for the PDP to map the MAC address of an IP address. This information can be extracted from the DHCP server, provided all the clients use DHCP assignment.

4.4 VI Case

4.4.1 802.1x versus SNMP detection

The differences between 802.1x and SNMP seem clear. 802.1x provides standard authentication services from design while SNMP detection lacks any. 802.1x however, requires 802.1x client software and configuration [7]. Implementations of registration capabilities (e.g. at the authentication server or switch level) based on only 802.1x traffic do not give an accurate detection and registration of non capable 802.1x clients. Taken into account the large number of guest systems and non 802.1x capable industrial automation equipment 2.4.3, SNMP detection is the most preferred technique when doing element detection at VI.

4.4.2 Mapping of MAC - IP addresses

The mapping of MAC - IP addresses through DHCP is no option for VI. Many industrial engineering systems make use of static IP addresses and have no capabilities to run DHCP, making DHCP static entries not an option. Other options to make this mapping possible could be:

- Inverse ARP
- Consulting layer 3 device ARP table
- Monitoring a mirroring port on the access device
- Manual registration

Inverse ARP
The requesting of IP information can be done through the use of Inverse ARP (InARP) [18], an extension to ARP mainly designed for WAN (frame relay and ATM) connections. InARP maps a given MAC address to an unknown IP address. In contrary to RARP, which is designed to resolve the requesting hosts IP address, this query can be for any other MAC address. The difference between InARP and ARP is that InARP does not broadcast requests because the hardware address of the destination station is already known. With no background information on any implementation of InARP in current network operating systems it remains to be seen how this protocol can be of any practical value.

Layer 3 ARP table
Another source of information can be the ARP table of a central layer 3 router or switch [19]. As described in section 2.4.1 the VI network is built around a collapsed core which contains two layer 3 switches. Provided the AR has communicated through the core router to another system (not just

on the local network) an ARP table entry is made with the MAC - IP match. This information could be collected by using the SNMP MAC Notification Trap [17] or by listing the "ipNetToMediaTable" MIB-2 class [20]. Unfortunately, it is no certainty that an AR will communicate through the core router with other hosts on the network. PLC's in VI's example just hold after startup, waiting for a high level system to initiate communication with it. Although this implies no infection problems to network parts reached through the core, it is possible to infect devices attached to the local layer 2 device.
The ARP table could be filled by pinging IP ranges on the registration VLAN. VI uses many IP ranges, sometimes also separate ranges for customer projects. In this solution, the IP ranges need to be manually updated and is therefore susceptible to faults. Next to that, pinging is to be done in cycles which could negatively influence the time the host can get access to production VLAN's.

Port Mirroring
Port mirroring, also called "roving analysis port" in some vendor implementations [21] is a switch port on which all egress and/or ingress traffic of all local or remote switch ports is copied. By issuing such a port on access network devices it could be possible with a layer 3 device to see the first connection setup on every switch port. The problem with this solution is its scalability. VI counts worldwide around 300 access switches which should be equipped with such a mirror port and listening device. Possible aggregation of this network traffic is no option due to high bandwidth demands on the aggregating channel and detection device. Next to this, it implies that a host always initiates traffic, which is not the case for PLC equipment at VI.

Manual Registration
It is possible to register MAC and IP addresses for static IP devices. This however presents huge administrative overhead and reduces the flexible use of IP addresses VI (mostly PLC engineers) are accustomed to. Next to this, it poses no matching for non-registered malicious static IP hosts who are able to quickly switch IP address.

4.4.3 Practical verifications

MAC address table entries
The main question about SNMP detection remains: is a MAC address table entry made when a computer is connected? This question has been verified in a test setup with a workstation running Windows XP and a Siemens PLC's connected to a layer 2 switch. Packets were inspected with Wireshark [22] on a port mirroring port. The following arguments are verified on both

the Windows and Siemens PLC IP stack when configured with a static IP:

- MAC address table entries are made when traffic is flown to or from the connecting host.
- Gratuitous ARP requests [23] are sent out when the IP Stack is initialized (NIC is connected or host boots up). Gratuitous ARP is designed to detect duplicate IP addresses and update other machines ARP tables with MAC or IP addresses. These are sent out on the broadcast address of the configured IP subnet.

The following arguments are verified on the Windows IP stack configured with a DHCP address assignment:

- When sending "DHCP Discovery" in order to acquire a DHCP address, the MAC is known due to the traffic initiated at the host.
- Gratuitous ARP are sent:
  - When starting up and no DHCP assignment has been possible; when supported on the "zeroconf" [26] (for Windows machines called APIPA) broadcast address (169.254.255.255)
  - When an earlier assigned address has not expired; on the broadcast address of the assigned IP address network.

Next to this, Windows machines send out local browser announcements [24] every 12 minutes on the broadcast address of the configured IP subnet. Gratuitous ARP can be disabled [25] on the connecting host and thus can be circumvented to do immediate detection. However, a MAC address table entry will appear when the first communication takes place. For these reasons, SNMP detection of a connecting host is a qualified technique to do element detection.

Mapping MAC - IP address
Since gratuitous ARP broadcasts send out the hosts MAC address and IP address, it presents a way to do the mapping of MAC and IP address for hosts. However, when verifying this possibility in the test setup, the gratuitous ARP broadcast (directed to the MAC broadcast address) was handled in the following different ways:

- When the IP address was initially set, the broadcast was received on all devices connected to the upper layer 3 (core) device.
- When the IP stack was initialized with a previous configured IP address or the host boots up, the broadcast was stopped by the layer 2 device.

When looking at the gratuitous ARP packets with a packet analyser, it showed *no* differences between the first and second broadcast. This suggests that the differences in handling are made by the layer 2 device although it is a layer 3 activity.
To include both situations in element detection, it is necessary to monitor the gratuitous ARP broadcasts on a port mirroring port on the local device. The disadvantage of this situation is the high bandwidth demands when port mirroring ports are aggregated. Also, gratuitous ARP can be disabled by an attacker.

Another plausible solution is the mapping of MAC - IP addresses from the central ARP table of a layer 3 device. The following arguments are verified on a test setup with a layer 2 connected to a layer 3 device network device and (layer 2) connected clients running Windows XP and Siemens proprietary IP stack. When configured with static IP devices the following arguments are valid:

- ARP table entries are made when traffic is routed over the layer 3 device to or from the connecting host.

The following arguments are verified on the Windows IP stack configured with a DHCP address assignment:

- ARP table entries are made when traffic is routed over the layer 3 device to or from the connecting host.
- When sending "DHCP Request" for renewal of the DHCP address the IP address is known due to the unicast traffic initiated at the host.

This technique poses no solution to match the MAC and IP address of a connecting static IP device that does not communicate over the layer 3 device. For these reasons, VI has the end decision between the following:

1. Do manual registration
    - Manual registration of MAC and IP address, this poses administrative overhead and non-detection of malicious AR's who are able to quickly switch IP address.
    - Pinging IP ranges, this poses administrative overhead for the maintenance of used IP ranges and due to the cyclic nature of the technique negatively impacts the time to detect connecting AR's.
2. Aggregate network traffic of the detection VLAN on a (remote) port mirroring port to acquire gratuitous ARP requests. This poses high bandwidth demands on the aggregating port. Also, gratuitous ARP can be switched off by the connecting AR and thus poses no protection against attackers who do so.

The end advice to VI in this circumstance is to keep manual registration of MAC and IP addresses in a database since it is anyhow necessary for static IP and non-browser devices to do a pre-registration to skip authentication. Malicious AR's who are able to quickly switch IP address could be detected by the numerous ARP table entries at the core layer 3 device.

5 Registration & authentication

A NAC solution needs to provide a way to register access of devices and authenticate users who plan to register these devices. This chapter focuses on the technical aspect of registration and authentication. The organizational processes on registration is outlined in chapter 10 of this report.

5.1 Registration

5.1.1 Repository

In order to administer who is responsible for an AR, a NAC solution should provide a way to couple user information to computer information. With this information, it should also be possible to perform role-based access to specific parts of the network. In order to perform user authentication, user information must be available. These can usually be derived from an LDAP user authentication repository. The only way to uniquely identify network equipment is by MAC address, as described in the element detection section (4).

5.1.2 Central based approach

In a central based approach, computer information is coupled with user information through a central administration body such as (a combination of) the IT department, human resources (HR) and visitor registration (i.e. building receptions).

5.1.3 User based approach

A central based approach clearly offers less flexibility to register devices. For locations where there is no visitor registration and direct IT support (e.g. support through phone) it is not an option to handle registration through an administrative body. For this purposes, it is possible to let users register network equipment themselves.

5.2 Authentication

5.2.1 Registration is authentication

It is possible to let the registration of the MAC address be the authentication of the client on the network. This however, poses the threat that a MAC address could be duplicated to obtain access on a non registered device.

5.2.2 802.1x

802.1x (4.4.1) offers users authentication through RADIUS. 802.1x is session based so authentication has to be performed every time a client logs on. Clients need to be equipped with an 802.1x client to complete authentication. Authentication can be performed through any EAP mechanism [27]. Depending on the chosen mechanism, authentication server and client could be required to have an X.509 certificate [28] or pass workstation login credentials.

5.2.3 Captive Portal & Registration VLAN

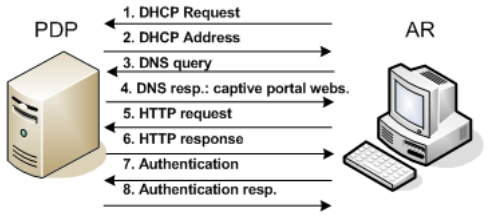


Figure 3: Captive Portal

Captive portal techniques must be used in conjunction with policy enforcement methods (see chapter 6) to have effect. With captive portals [17] the user is ”caught” on a webpage when it tries to use its browser. Systems with no browser or an active user controlling it (e.g. servers) should be registered in pre advance to exclude them from this process. The captive portal authentication could be done once (e.g. registration of future legitimate use of the switch port/MAC address combination) or session based (e.g. every time the host boots up at the switch port). Figure 3 outlines the scenario for DHCP capable AR’s in the registration VLAN. First (1) the client requests a DHCP address. The PDP or an other DHCP server is configured to answer this request with an IP address assignment in the registration VLAN (2) with an own, custom DNS server address (possibly running on the PDP itself). Next, the user on the AR starts up a browser and does a random DNS lookup query (3). The PDP responds with the IP address of a custom web server (4) where the captive portal is hosted and user credentials or certificate can be verified (5,6,7,8). Authentication should be conducted over a secure communication channel such as Transport Layer Security (TLS) [30].

5.3 VI Case

5.3.1 Registration

Registration should be performed on a user based approach. This is mainly due to the loose security policy now in effect for users of VI's IT environment. This policy ensures users that they can connect a wide variety of (customer) network equipment at any place, at any time (e.g. in different timezones where there is no IT support). During the questionnaire with IT management it came clear that users are used to this loose security policy and thrive on the freedom the IT environment provides them (see also 2.1). Also, a central based approach would cause administration overhead due to the information that needs to be filled in and kept up-to-date. Users information can be imported from the central LDAP user directory where all (external) employees are kept up-to-date. By linking the user information with computer information, it is possible for the NAC solution to inform the responsible person when necessary.

5.3.2 802.1x and captive portal VLAN

The main difference between 802.1x and captive portal techniques is the moment of authentication. 802.1x has default implementations of the authentication client in common operating systems such as Microsoft Windows 2000 SP4 and later [29] which include the operating systems mostly found on office automation systems at VI (see also 2.4.3). This enables 802.1x to authenticate the AR when the AR boots up or user logs on. By using a captive portal, this authentication is done after the user logs on when firing up a browser. A captive portal also requires SSO techniques (e.g. Kerberos) to skip re-authentication for LDAP authenticated users. On the other hand, captive portal techniques could become useful when providing the user instructions to cure his machine. Strictly spoken, there are two ways an AR can be authenticated in 802.1x and captive portal environments:

1. By client certificate: requires no to minimal (password to access smart card in case of user certificate) extra user input.

2. By user LDAP credential pass through: requires no extra user input.

Currently, there is no Public Key Infrastructure (PKI) deployed at VI. There are future plans to deploy a PKI to facilitate smart card based user authentication which could then be integrated with NAC. For the moment however, credential pass through (given at workstation login) should suffice. To facilitate non-administered clients and non-802.1x supported clients, it is necessary to have a captive portal in effect. When used in conjunction with 802.1x, the captive portal should be placed in a separate VLAN where

clients are to be placed when 802.1x authentication could not be performed or fails. Combining both techniques requires that 802.1x must be integrated with the captive portal to allow 802.1x AR's to skip captive portal authentication and continue with pre-admission scanning. The authentication of static IP and no browser clients is outlined in section 5.3.4.
Appendix B (58) and C (59) outline an overview of the authentication scenario in 802.1x and captive portal. It is clear that 802.1x makes the authentication scenario extra complex since it is an extra stage in design an build of the system. The end advise is to only use captive portal techniques since this reduces the complexity of the system and provides a generic way of authentication to all AR's except static-IP and no browser systems.

5.3.3 Guest Users

A captive portal offers flexibility to non-registered guest systems. Through the captive portal it is possible to make an option to only continue to a "guest network" state thereby continuing to the pre-admission scan, but when admitted have limited access. With this "guest network" option, it is possible to request user information which is then dispatched to an administrative body. This option could be restricted by requiring a login account issued by a guest sign-in desk (e.g. reception). Although this sounds like a reasonable proposal, VI currently holds no visitor registrations at their offices. It is therefore unrealistic to demand registration only for IT purposes. When required, it should be possible to disable access to the AR by denying its MAC address. In the end, it is still possible to change the MAC address and regain access to the guest VLAN. By pre-administrating guest users it should be possible to, if necessarily required, allow guests to the production network through the captive portal. This functionality should nevertheless be used with care since it exposes the entire network to a non corporate employee. Role based access should be in place to further bound the users ability in production environment. Specification of roll based access goes beyond the scope of this advisory report.

5.3.4 Static IP clients & no browser clients

By choosing for authentication through captive portal, industrial automation equipment cannot be authenticated simply because these are not equipped with a browser. Next to this, static IP devices are probably not configured with the NAC DNS server. As outlined in section 4.4 static IP devices are to be registered in pre-advance with their MAC and IP address. This registration should enable them to skip authentication and get them to the next phase of NAC, pre-admission control. Although this poses the hazard of MAC address spoofing [16], it is possible with pre-admission scans to identify some other unique elements of a computer. (i.e. the OS running on it).

If the pre-admission scan discovers great mismatches in the elements of the previous scan and the new scan, it should deny the AR access. This deny can after wise be reset by administration of the NAC after verifying what caused the mismatch. It is alway possible to exclude access switches in secure environments from the solution such as those in server rooms.

5.3.5 Extra network equipment

At VI, it is permitted for users to add extra network equipment to the network (e.g. to spread the number of available network connections). This network equipment can be issued by IT or bought/brought in by users (mostly engineering employees). These devices should be used sporadically because, without administrative access to the access device, it is impossible to enforce policies on the client. An organizational policy on this subject (see also 10.1.4) should be in effect. In the NAC solution it should be possible to make an exception by MAC address. This exception will exclude the network device from the NAC process.

5.3.6 Administrative access

When authentication is performed for production VLAN users, administrative access to the AR is required in order to check policies by post-admission control. To obtain administrative access to guest user systems, a dissolvable agent should be hosted on the captive portal site. A user who wants to enter production VLAN's with a machine that does not accept administrative LDAP credentials first has to install this agent. The back end system should check administrative access upon authentication of the user - AR combination in the captive portal. Pre-registered MAC addresses should be excluded from this check.

6 Policy enforcement

The next step in the sequence to NAC is to choose a way to enforce policies for the Access Requestor (AR) [7]. The goal of policy enforcement is the action in response to a hosts state. This enforcement can be done in various ways [9] which are discussed below.

6.1 802.1x

In extension to section 4.4.1, 802.1x provides two enforcement environments. The ”unauthorized” state and the ”authorized” state are enforced at the access device (switch). In the ”unauthorized” state only authorization information is allowed to pass through the switch to the defined authorization server. In ”authorized” mode, all network traffic is allowed to pass. Vendor modifications to the protocol however, [31], [32] add the possibility of a ”guest VLAN” when 802.1x authentication is not possible or fails.

6.2 ARP

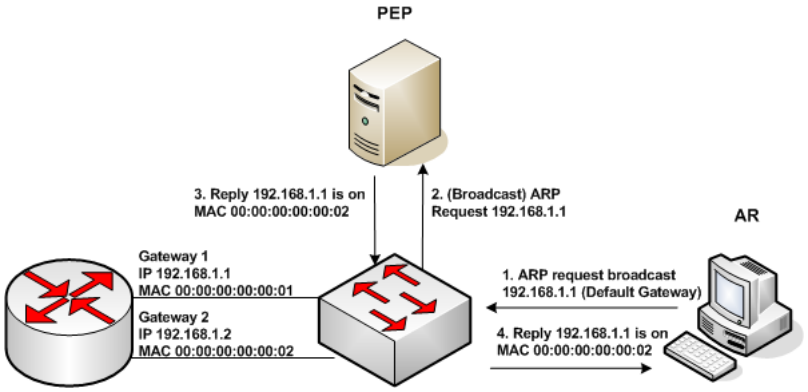


Figure 4: ARP influencing

Address Resolution Protocol (ARP) [33] can be used to influence the traffic direction on a layer 2 network. Figure 4 outlines the scenario, mainly derived from ARP ”poisoning” techniques [34]. First (1) an AR sends out an ARP request broadcast to lookup its default gateway. On policy decision, a locally attached PEP may reply to this broadcast (2) with the MAC address of a different gateway (3,4). All AR’s traffic will now be switched to the PEP’s specified gateway. With this modified gateway it is possible to remediate the enforced client, possibly by extending the (captured) environment behind the gateway with VLAN’s to remediation services. This solution has many disadvantages:

- Hosts on the local LAN are susceptible to cross contamination (e.g. computer worms).
- There must be intelligence connected to every local network.
- ARP broadcasts can be replied to by every client on the local network. While ARP works by the concept of ”first come first go” this technique gives no hard guarantees unless the switch or all other clients or are configured to not respond or let only the PEP respond to ARP requests.
- Steering is difficult in this technique because ARP table entries are held on clients for a specified caching time or during a workstation logon session. If network traffic continues to flow this entry will not disappear. Because of this reasons, the PEP has no means to re-route traffic to the ”correct” gateway when the AR is cured. One possible solution for this could be to let the traffic flow through the PEP itself for remediation purposes and afterwards serve as a ”normal” gateway. The problem with this setup is, that if the ARP cache entry stays at the client, the PEP could serve lots of traffic thereby negatively influencing the performance of the network.

6.3 In-line devices

In-line devices could be placed in the network between all uplinks of the access layer switches to the upper layer (core) network. The in-line device in this situation can serve as a PEP but can also be used to examine passing traffic. The problem with these devices is often that the device cannot handle the required bandwidth and latency on uplink connections. This solution also needs many locally deployed devices on uplinks and provides no measures against cross contamination by computer worms on the local network.

6.4 DHCP

Dynamic Host Configuration Protocol (DHCP) [35] also provides means to steer the network environment of an AR. By making the PEP the DHCP server, it can provide a different subnet configuration for AR’s who need remediation. By configuring layer 3 devices with Access Control Lists (ACL’s), it is possible to capture a client in a remediation environment. DHCP provides no solution to cross contamination. Next to that, when a hosts needs to be placed in a different environment, there is no way to ”force” a DHCP request from the AR. A solution for this could be to keep the DHCP leasing times very short. This will unfortunately result in massive broadcasts

on the local network for DHCP renewals. Also, this solution provides no means to enforce static IP devices.

6.5 Dynamic VLAN

Provided the network access device (i.e. switch) supports this technique, dynamic VLAN assignment through SNMP can put the traffic of an AR on a separate (remediation) "LAN", thereby isolating the contaminated client from the clients. Provided VLAN information is distributed through all LAN network devices (e.g. with protocols such as VTP) it is possible to include remediation services servers on the VLAN.

6.6 Administrative access

Administrative access provides more insight to the conditions of software running on an AR. With administrative access, it is possible to:

- Check the AR for installed programs
- Determine the patch level of the operating system and antivirus products.

Administrative access is usually obtained through a software agent. For AR's in an organizations domain this agent can be installed through software policies. For guest AR's this can be done through dissolvable agents [9]. The downside of dissolvable agents is that they are usually made for common client operating systems [9] and require the user running it to have administrative access himself. Another way to obtain access is through an automated network software scanner running from the network. These scanners however require administrative credentials on the users computer, something guests will not give away very likely due to legislation of the guest systems owner.

6.7 VI Case

6.7.1 Policy enforcement

Policy enforcement is preferably done through dynamic VLAN's assignment after the 802.1x process. ARP and in-line devices require, next to their individual disadvantages mentioned in the previous section, the presence of intelligence on every access device. DHCP or Dynamic VLAN assignment do not have this requirement but offer no protection against cross contamination in a remediation environment. Cross contamination could be mitigated by placing all AR's in their own VLAN. There are two possible techniques to arrange this:

- Assign random VLAN numbers.
- Use private VLAN's.

6.7.2 Assign random VLAN numbers

By letting the PDP assign the PEP a random VLAN number, it isolates the AR from the rest of the isolated AR's. To make the remediation services accessible to the client, this VLAN also needs to be routed through the core of the network to the remediation service. Access ports for servers which contain remediation services should trunk traffic [36] with protocols such as dot1q [37]. The remediation servers should be configured to reply with the VLAN tag the request came in.

6.7.3 Private VLAN

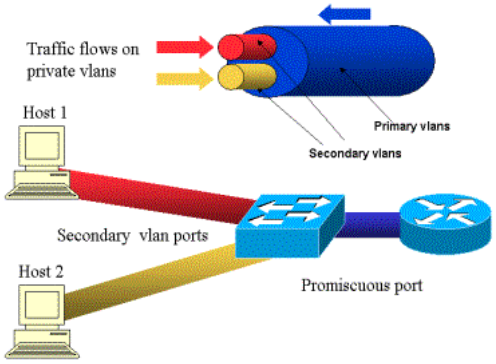


Figure 5: Private VLAN
Copyright Cisco Systems [38]

Private VLAN (PVLAN) [38] is a proprietary functionality developed by Cisco Systems mainly for DMZ and internet service providers purposes. With PVLAN it is possible to communicate with hosts in a primary VLAN but not let hosts communicate with each other when connected to a single access device. As displayed in figure 5, when using the PVLAN model, AR's are placed in VLAN's defined as "secondary" and "isolated" at the layer 2 access device. Remediation server access ports are placed in the primary VLAN (defined as promiscuous port), receiving data of all mapped secondary VLAN's. This setup reduces the number of configured VLAN's throughout the core network and does not require VLAN tagging at the remediation servers. Traffic back from the servers is tagged with the primary VLAN identifier and can be received on all mapped secondary VLAN's. It

has to be mentioned that this option is only available on Cisco based networks with specific series of hardware equipment and software versions [38]. Next to that, VTP has to be configured transparently on all switches participating in the setup.
Since VI's network is built around PVLAN capable equipment, 802.1x with PVLAN provides the best options for easy configuration of policy enforcement. It has to be mentioned that this choice has to be made by taking future plans into account. If VI has plans to buy non PVLAN supported network equipment it is better to choose for the "random VLAN assignment" option. When the remediation and/or authentication services are virtualized VI needs to take into account that the possible use of virtual switches will not support this proprietary function. Also, VI has to take into account that VTP functionality must be disabled when deploying PVLAN. To remediate this, VLAN changes should be distributed by others means such as switch configuration deployment software. 802.1x vendor extensions for guest VLAN's [32] do not offer the same functionality with PVLAN. It is therefore necessary to let the PDP do the switch port configuration after the 802.1x authentication with SNMP commands.

6.7.4 Administrative access

The questionnaire with the IT department at VI pointed out that it does not want to consider a goal of NAC to enforce software policies. Therefore, administrative access should be limited to checking the patch level of the operating system and anti virus products and severe vulnerabilities in installed software products. One practical way to verify this is with the use of the network scanner Nessus [39]. When provided with administrative credentials, this scanner is able to verify what updates have been applied to common operating systems such as Windows which is commonly used at VI (2.4.3). The problem remains to obtain administrative access to guest user systems. For this purpose, a dissolvable agent should be hosted on the captive portal site. A guest user first has to install this agent in order to let NAC verify policies.

6.7.5 Practical verifications

In order to make use of dynamic VLAN assignment, it has to be verified that the client renews the DHCP address when the VLAN is set (changed) on a switch port. The following arguments are determined on a test setup with a layer 2 switch connected to a layer 3 switch. On these switches, 2 VLAN's were assigned of which one contained a generic DHCP client (Windows OS) and the other contained a DHCP server (Windows as generally deployed at VI). At the VLAN containing the DHCP client, the IP-helper address was configured to forward DHCP broadcast of the client to

the DHCP server. The DHCP lease time was set to 90 seconds. The following argument is true when allocating the switch port to a new VLAN:

- When switched, the DHCP address was renewed immediately after the expiration of the address. (normal behaviour)

The following argument is true when allocating the switch port to a new VLAN and issuing a shutdown and start up of the switch port within 5 seconds:

- When switched, the DHCP address was renewed immediately after the start up of the switch port.

Previous arguments are also valid when using PVLAN's. When PVLAN's ports are to be switched to other environments, they can simply be mapped to an other primary VLAN. These arguments result in the conclusion that issuing a shutdown/start up command after VLAN allocation has a positive effect on the DHCP renewal time of the client.

7 Pre-admission evaluation

The goal of the pre-admission evaluation stage is to check the health of a connecting AR before it may enter other sections of the network. This process is usually done through a vulnerability scan and monitoring the AR's network traffic [17]. Pre-admission scanning is done in a limited access environment and disables the users' ability to access the required network resources to do his job. It is therefore essential that the time-to-completion of a pre-admission evaluation stays below a user acceptable timeframe.

7.1 Vulnerability scanning

Vulnerability scanning provides means to check a host on all kinds of threats which can vary in severity. To provide a network based approach it is essential to invoke this scanning from a network station located in the pre-admission VLAN. After vulnerability scanning is completed, this report information should be exchanged with the PDP. Next, the PDP can classify the host based on this report and authentication information.
Vulnerability scanning when having administrative rights on the client machine greatly improves scanning results. With administrative rights it is possible to list software installed on the machine and determine patch level of the operating system and virus scan software. With this information it is possible to determine specific threats on the software.

7.2 Intrusion detection

Intrusion detection plays an import role in the pre-admission phase. Since cross contamination usually happens through data traffic, by first analyzing the traffic during pre-admission it should be possible to determine that an AR produces no malicious network activities.

7.3 User interaction

User interaction is essential in the pre-admission stage of a NAC solution. Since a non-client based approach cannot force any cure on the AR, the user should be provided with instruction to do so him or herself. When pre-admission scan classifies the AR as a potential threat, a captive portal deployed in the remediation VLAN could provide the user with instructions. Scanning information should be exchanged about the detected vulnerability. Instructions to solve the issues should be written in advance and mapped to different classes of vulnerabilities. After the issues have been solved, it should be possible for the user to re-scan its machine after which it can be placed out of remediation environment.

7.4 VI-Case

The level of threat accepted in pre-admission phase strongly correlates with the accepted scanning-time. While this stays a security management issue, questionnaires with IT management pointed out that 30 seconds is an acceptable time-to-connect. Appendix A (see page 57) displays the threats VI equipment is exposed to. To keep within the stated timeframe it is essential to only include active network security threats in the pre-admission scan. These threats must be severe to other clients placed in the same production VLAN (e.g. cross contamination). Non-severe threats should be noticed by post-admission scans after which, dependable on the severity, re-classification of the AR could occur.
Because non-802.1x authentication and remediation is performed in a single VLAN, this poses a threat to the availability of the authentication services. It is therefore necessary to protect the captive portal. This could be done by only admitting HTTPS traffic to the captive portal server. Also, the captive portal website itself should be secured against standard web server threats and input threats. Exact technical solutions are beyond the scope of this report.

7.4.1 Vulnerability scanning

Vulnerability scan advisory (in pre- and post-admission stage) is based on the Tenable Nessus [39] vulnerability scanner, who has a top 20 listing for security tools according to sectools.org. Nessus encompasses at the moment of this writing 24887 plug-ins in their ProfessionalFeed commercial version, covering 9741 Common Vulnerabilities and Exploits (CVE's) [40]. Threats that should be addressed during pre-admission scanning are all Nessus plug-ins classified as "backdoors" [41]. These backdoors or "worms" are a hazard to other AR's in a production VLAN environment. Nessus ProfessionalFeed also encompasses 32 plug-ins for known exploits on SCADA equipment (industrial automation systems) [42] which could be used to check VI SCADA equipment on vulnerabilities. Only AR's with vulnerabilities marked as "high" should be forced by the PDP to stay in the remediation environment as these pose immediate threat. Vulnerabilities with "medium" classification should be reported to the end-user by mail as they are not immediately exploitable but could cause future trouble.
For authentic user AR's it is now necessary, with administrative privilege, to check the operating system patch level and antivirus patch level. These latest patch levels should be the patch level required by IT management in order to get access. Also, Nessus should be kept up to date with the latest plugins in order to check on the latest vulnerabilities.

7.4.2 Intrusion detection

The intrusion detection advisory is based on Snort [43] who is, just like Nessus, among the top 20 listing for security tools according to sectools.org. Intrusion detection can be implemented at VI on a port mirroring port (4.4.2) on a core layer device in the network. On this port, all network traffic from the pre-admission VLAN is copied from the dynamically mapped PVLAN ports of AR's in pre-admission stage. Snort can handle throughputs around 125 Mbit/s [44] while some speak of 200 Mbit/s [45] which is a design limitation. Although multiple hosts could interfere the correct working of the IDS by producing a lot of network traffic at the same time, traffic could be limited on a switch port basis to prevent such a situation [46]. Snort employs rule sets (categorization) which contain rules of the set type. Snort should be run with the default rule sets active as displayed in Appendix C (59). Also, the "backdoors" and "virus" non-default rule sets should be activated to cover endpoint security threats (see also 57). Snort classifies the priority of a rule violation [47]:

- Priority 1 - High Priority Classifications (e.g. A Network Trojan was detected)
- Priority 2 - Medium Priority Classifications (e.g. Potentially Bad Traffic)
- Priority 3 - Low Priority Classifications (e.g. Detection of a Network Scan)

For pre-admission scanning, different priorities can be mapped to different users categories. Guest users should be required to fix only priority 1 violations, as priority 2 and 3 pose no immediate threat to other AR in the guest VLAN. Authenticated users for production VLAN's should be required to fix priority 1 and 2 violations, mainly due to the danger these violations (can) host to production VLAN services. The fine tuning of Snort goes beyond the scope of this report, but the interested reader is referred to [48] and [49].

7.4.3 User Interaction

While captive portal functionality serves the possibility of the user fixing the problem itself, it provides no means to cure pre-registered hosts (i.e. static IP devices and non-browser devices). For these AR's, it is essential to also pre-register a way to communicate with the responsible owner. When a threat is detected, the threat and possible cure action should be communicated by media such as email or mobile SMS. With these communication media, the user is informed real-time on the limitation in effect on his/her AR and the possible solution to fix the problems. It should be possible to

initiate a re-scan by answering the mail, SMS or by logging into the pre-registration portal.

7.4.4 Known MAC allowance

Pre-admission evaluation could be problematic in terms of the ”time to production” when an AR is rebooted multiple times. According to PLC engineers of VI, this is common practice on industrial hardware. It is therefore possible for the PDP to verify if a MAC address reappears within a certain threshold on the same switch port and passed pre-admission scanning before (within this threshold). If this threshold is kept within an arbitrary amount of time it is highly unlikely the client could have been infected by other ways. While this still poses the threat of an attacker re-appearing within the threshold with a malicious host with a spoofed MAC address on the same port, this should be a security versus usability security management decision by VI. It is advisable to only implement this functionality for pre-registration devices which are, for the most part, industrial automation hardware. Post-admission evaluation in this situation should be considered safe enough to detect misuse of this functionality.

7.4.5 Pre-register MAC

The pre-registration of static IP devices and non-browser devices poses a threat concerning MAC address spoofing. Pre-admission evaluation can be configured to save unique elements (e.g. operating system and computer name) of the pre-register devices to a database. When a new evaluation points out differences between the database and the current AR, access should be denied.

7.4.6 Practical Verifications

Practical verifications in this section are the completion time of the vulnerability scan and monitoring standard PLC traffic to check if Snort marks any normal network traffic as suspicious.

Scanning time Nessus
The following arguments were verified on a test setup featuring a production layer 2 switch with a connected Nessus 3.2.1.1 vulnerability scanner. Vulnerability scanned hosts were standard Windows XP SP2 deployed at VI, a Profinet based PLC test setup and Unix-based QNX.

Computer network worms
When the proposed ”backdoor” category was enabled, scanning times were the following:

- On standard desktop machines (Windows XP) 1:20 minutes and 1:30 minutes.
- On PLC equipment: between 2:00 minutes and 2:30 minutes.
- On FSC (QNX) equipment: between 1:30 and 1:40.

These scanning times are beyond the VI acceptable 30 seconds (7.4). It is therefore advisable to only inspect network traffic with Snort during pre-admission evaluation. Since a computer network worm must expose network traffic to infect other clients, Snort scanning should detect this.

Administrative checks
When the proposed administrative access category was enabled, scanning times on standard desktop machines (Windows XP) were between 15 and 16 minutes. These scanning times are also far beyond the VI acceptable 30 seconds. It must therefore be verified if it is possible to check the patch level of the operating system and antivirus product through remote scripting. If this is not possible, post-admission scanning on this feature should be considered. In the end, installing a(n) (dissolvable) agent on all machines is an option although this is against a network based NAC approach.

IDS PLC Test
The following arguments were verified with Snort 2.8.3.2 connected to a port mirroring port on a layer 2 switch. Also connected to the switch was a Profinet based PLC test setup and a management station running Windows XP SP2. In the test setup, normal network activities were run such as the loading of configurations and accessing the (optional) webservice of the PLC test setup. The only traffic detected as malicious was an "EXPLOIT RealVNC server authentication bypass attempt" which was caused by a VNC service running without password on a Windows CE machine used to display PLC information.
The conclusion of this test is that there are currently no "strange" network activities detected by the proposed security ruleset of Snort on standard PLC network activities.

8 Access classification

Access classification is the process after the pre-admission evaluation when the AR is bound to a certain environment. This classification is dependable on authentication and results of the pre-admission evaluation. Also, post-admission control in the production environment may force an AR to re-bound to the authentication & remediation environment. Since the completion of the environments is IT policy dependable, this chapter will solely deal the VI case.

8.1 Authentication & remediation environment

The authentication & remediation environment is the "starting" VLAN where AR's are authenticated and possibly cured. An AR will continue to stay in the authentication & remediation VLAN when the pre-admission scan points out that there are severe threats (see also 7.4) of the requester. Also, if post-admission scanning points out that an AR poses a severe threat to the network or to itself, it will be bound to the authentication & remediation VLAN. The authentication & remediation VLAN is build around individual PVLAN's (6.7.3) bound to a main VLAN. This main VLAN has to block access to other VLAN's (i.e. production/guest VLAN's). Services that should be in placed in the main VLAN include:

1. Critical network services
2. Pre-admission evaluation
3. OS update services
4. Antivirus services
5. General application services

These services must be highly protected due to the (possible) hazardous clients on this VLAN. The services must be hosted on servers dedicated to the VLAN to prevent cross contamination.

1. Critical network services
Critical network service on the VLAN include:

- Internal DNS services
- DHCP services
- Hosting of the captive portal to redo authentication

2. Pre-admission evaluation
Pre-admission evaluation as described in the chapter 7 should be in effect on the authentication & remediation VLAN to check the health of a connecting AR.

3. OS update services
OS update services in the VLAN should contain critical updates on all common operating systems deployed in the organization (2.4.3). Examples of these services are Windows Software Update Services (WSUS) for Windows machines and repository services for Linux. It should be mentioned that it is not possible for a user to execute these updates when he or she has no administrative rights on the AR. Since IT questionnaire during this research pointed out that around 80% of VI's employees have administrative rights on their workstation, this should not be a problem for VI employee users.

4. Antivirus services
The current antivirus services deployed at VI comprise a corporate virus scanner 2.4.5 installed on all Windows OS workstations. While it is possible to host an update repository with McAfee DAT files (virus definitions), administrative control over the virus scanning software is needed to change the update repository location. A better solution, also available to guest users, is to provide a separate virus scanning and removal tool. An example of such a tool is "Stinger" from McAfee [50].

5. General application services
General applications (i.e. Adobe Reader, Java Runtime Environment) may also pose vulnerabilities to AR's. These vulnerabilities must be detected by the vulnerability scanner deployed in the production environment. The configuration of the general application repository should depend on IT management policy. There can be two options:

1. Host a repository with standard applications
2. Give limit access to a list of mapped websites

1. Repository
A repository should host a list of the newest freeware applications of which old version may contain a threat to security. Although such a repository requires extensive maintenance and may bring legal issues, it is possible for the user to install a new version of the application not posing the vulnerability.

2. Limit access to mapped websites
It is possible to supply limited access to patch websites based on programs

listed in the Common Vulnerability Exposures (CVE's) [40]. This requires a proxy server and an intelligent DNS server to limit the user's accessibility to the Internet. Also, the list of accessible websites should be manually maintained or a link between the CVE's and known websites must be build.

8.2 Guest environment

An AR will be placed in the guest VLAN when the user has selected guest access on the captive portal website. This VLAN has to block access to other VLAN's (i.e. production/remediation & authentication VLAN's). When choosing for a high secure environment, it is possible to choose for individual PVLAN's in the guest network. VI however wants to enable local area networking in guest VLAN to facilitate subcontractors. The services that should be in place on the guest VLAN include:

1. Critical network services
2. Internet connection
3. Post admission scanning services

Re-classification of hosts to the remediation VLAN can be done by vulnerability scanning and IDS.

1. Critical network services
Critical network services on the guest VLAN include:

- Internal and external DNS services
- DHCP services
- Hosting of the captive portal to redo classification

2. Internet connection
The Internet connection on the guest VLAN should provide limited access depending on the stated policy by IT management. This is done for guest users (e.g. subcontractors or customers) that only seek connection to their home (company) network. (e.g. through SSL VPN). It is advisable to only limit the traffic to well known, policy acceptable, ports.

3. Post admission evaluation
Post admission scanning services will continuously watch the behavior of AR's in the guest environment and is described in section 9.1.

8.3 Production environment

An AR will be placed in the production VLAN when captive portal authentication is successful, pre-admission scan points out there are no severe threats and there is administrative control over the equipment. Production VLAN's are currently deployed at VI and therefore require no further description of services. The next chapter will describe post-admission scanning which will be deployed in the production VLAN.

8.4 Wrap up

Now the access classification is outlined, the NAC solution can provide access to a user. In Appendix C on page 59 a flowchart is outlined with a complete view on the authentication procedure. Appendix E on page 62 depicts an overview of the different environments.

9 Post-admission scanning

Post admission scanning is the process of continuously verifying the health of an admitted AR. If required, the PDP can choose to reconfigure access of the AR by placing it into remediation. Post admission control differs from pre-admission control in the configuration of the detection elements. Since post admission control is a continues process that does not effect the users ability to work, it has no time limit boundaries as pre-admission evaluation. The remediation environment will not be discussed during this section, since there will be no post admission control in effect in this environment. Guest network and production network post admission control however, will differ. Since post admission control techniques are identical to pre-admission evaluation techniques they have already been discussed in chapter 7. Therefore this chapter will solely deal with the VI case.

9.1 Guest environment

The basic principle of the guest environment is that clients are checked on threats they pose for the network and to each other, but not to themselves (e.g. local viruses). This standpoint results from the policy that company data and its users (working in the production environment) must be forced to have a basic set of security measurements (1.1) and not every guest user, since they do not have direct access to company data. The guest network will have the same configuration on vulnerability scanning and IDS as the preadmission phase of the authentication & remediation VLAN (see 7.4).

9.2 Production environment

9.2.1 Vulnerability scanning

The basic principle of the production network is that clients are checked for threats posed to the network and to themselves. In order to do so, administrative rights have been verified (5.3.6) during authentication. Also, preadmission scanning pointed out if the patch level of the operating system and antivirus scanner is up-to-date. Vulnerabilities in common software running on the AR can now be checked.

Pre-registered AR's typically do not have an active user controlling them. This category normally contains server systems and SCADA equipment (2.4.3). To exclude both categories from administrative access is not preferred, since server systems may host vulnerabilities as well. Therefore, it should be possible to test systems in this category on an if-possible basis to access them with administrative credentials.
Since the pre-registration of MAC addresses poses the threat of MAC address spoofing, post admission control could be used to collect unique el-

ements of a host. When elements stored in the database differ from the elements now detected when scanning the AR, it is possible to block or limit access of the pre-registered MAC and send notification alerts to systems management.

Vulnerability scanning in the production network can be configured to check all listed plugins [41]. In case of Nessus this must be conducted in ”safe mode” meaning that on devices which are known to be adversely affected by denial of service attacks, these tests are not conducted [51]. Only ”High” vulnerabilities should force an AR back to the authentication & remediation VLAN where they can be cured. ”Medium” vulnerabilities and their solution are send through mail as they do not pose an immediate threat. All vulnerabilities detected on pre-registered machines (5.3.4) should be communicated to the registered user by mail, SMS or other real-time media.

9.2.2 Intrusion Detection

The Intrusion Detection System configuration for post admission scanning is the same configuration as the pre-admission (7.4.2) IDS configuration. However, in production, the Snort throughput limit of 125 Mbit/s [44] to 200 Mbit/s [45] prevents Snort from being the deployed in the core of the network. Currently, the core of VI's network has an average utilization of 380 Mbit/s when measured over 2 hours (daytime) with peaks of 650 Mbit/s when measured over 2 minutes (daytime). To enable full inspection of all network traffic, hardware accelerated Snort [45] or vendor IDS modules [52] directly connected or plugged into the core layer devices should be considered.

10 Organizational processes

An introduction of NAC largely depends on the organizational processes and policies surrounding it. In this section, organizational requirements to VI will be discussed.

10.1 Registration & Authentication

10.1.1 Registration limits

Since the proposed NAC architecture has a user based registration approach, registration limits must be in effect to limit the amount of machine registrations per user. This is also to safeguard the effective usage of the guest environment. Otherwise, every guest could be registered by a VI employee and is able to access the production network.

10.1.2 Pre-registration

Because pre-registration machines skip the authentication phase of the proposed architecture, this should be a limited available option. In normal circumstances, the following groups need to pre-register network equipment:

- Engineering departments: for PLC and SCADA equipment (2.4.3)
- IT department: for server management
- R&D department: for testing purposes

10.1.3 Authentication

When hardware is dispatched by IT to VI employees, the hardware is coupled to the user account by means of an employee number. With this link it is possible to determine the amount of seamless authentication attempts. When authentication is performed, the user is coupled to a specific machine for that session. When the session is over, the coupling ceases to exist. With this coupling it is possible to dispatch information about the AR to the responsible person.

10.1.4 Extra network equipment

A policy must be determined on adding extra network equipment (see also 10.1.4) to the network. If this network equipment is not configured by IT management, it will not participate in the NAC process. Therefore, extra network equipment should be kept to a minimum. Only qualified IT management (e.g. of the NAC system) should be able to add exceptions to the NAC system. These exceptions should be time bounded. The excluded

equipment must be replaced by IT configured network equipment as soon as possible.

10.2 Asset management

Currently, there is no asset management in place. Although general IT hardware (e.g. desktop, server systems) are issued by the IT servicedesk, other hardware (e.g. industrial automation computers) are not registered at all. In order to only pre-register company equipment, an asset management process is required. This process also requires intensive maintenance due to the nature of some systems. Systems are sometimes used internal during design phase and are eventually sold to customers.

10.3 Management effort

The NAC architecture described in this document is based on a low effort management design, mainly due to the self-service authentication and remediation. Activities that need to be performed from system management include:

- Checking a limited set of Common Vulnerabilities and Exposures (CVE's) on a frequent basis [40] and determine if they are a hazard to current systems.
- Keeping the remediation environment up to date (e.g. examine patch level).
- Maintenance of the pre-registration MAC list (e.g. possibly delete entries which are not used over a specific amount of time).
- Keeping the user instructions up to date.
- Fine tuning the pre and post- admission elements.
- Analysing trends.
- Perform manual interventions when policy misuse is detected.

Expectations are that these activities will lead to 0,3 FTE of effort by IT administration staff on the location Veghel. This is based on a total of 2300 devices connected to the network at the location in Veghel 2.4.3.

Activities that need to be performed by helpdesk staff include:

- Solving user problems when "self-solve" instructions provide no solution.
- Perform user registration in dialogue with human resources.

Expectations are that these activities will lead to 0,8 FTE of effort by helpdesk staff on the location Veghel. This is also based on a total of 2300 devices connected to the network at the location in Veghel 2.4.3.

During enrolment of the architecture, the effort will exceed these estimations. This will be mainly caused by the none-regulation now, user-awareness creation and fine tuning of the pre and post admission elements.

10.4 Hardening clients

Current policies on the hardening of IT network clients do not exist. For NAC, it is essential that the current situation is up to date, before the solution is deployed. Otherwise, users will be forced to fix the problems of the IT department. Operating system updates are currently deployed on an manual basis through software policies. While this provides no guarantees on deployment, an IT process which includes the testing of updates should be incorporated. Also, normal software updates are currently only deployed when there are usability problems with the software. In order to keep clients secure, IT management should check on vulnerabilities of current software. This could be done by checking a limited set of Common Vulnerabilities and Exposures (CVE's) on a frequent basis [40].

11 Conclusion & future research

A network based NAC architecture for VI poses the necessary demands. It is clear that NAC solutions can be company dependable, mainly derived by the nature of the users, working environment and connecting Access Requestors (AR's). Also, various improvements are possible when using different, sometimes vendor specific, techniques.
Reviewing the stated research questions from chapter 1:

What is the best architecture for a NAC solution in this environment?
Described in the different chapters of this advisory report, it can be stated that a NAC architecture for VI must have the following elements:

- Perform element detection through SNMP queries and traps.
- Authenticate users through captive portal techniques.
- Pre-register exception devices.
- Perform pre and post- evaluation checks to detect malicious behavior to the network or other clients.
- Evaluate the safety of the host itself by checking the state of installed software.
- Perform access classification dependable on the state and authentication of the AR.
- Provide remediation services and instructions for the user to cure the situation when necessary.

What elements and services should be part of this architecture?
Elements and services that should be in place to provide the necessary techniques are:

- General network services as DHCP and DNS.
- SNMP communication services (e.g. for VLAN assignment)
- Authentication services.
- Software, antivirus and operating system update repositories.
- Intrusion detection systems to verify malicious network activities.
- Vulnerability scanners to verify malicious network activities and evaluate AR's own safety.
- A dissolvable agent to evaluate AR's own safety for use on guest systems.

What organizational processes should be in place for an introduction of this technique?
The architecture focuses on the self-service aspect of the user by self authentication and registration bounded to a limited amount of authentication or registrations. Organizational processes 10 that should be implemented include asset management, limited registration of extra network equipment, the hardening of clients, administration of the solution and helpdesk support for the user.

Is network based NAC feasible technology for this situation?
The answer to this question is yes, but network based NAC alone does not provide enough information. As can be read in section 5.3.6, administrative access is required to determine the exact state of installed operating system updates, antivirus versions and malicious installed programs. For this reason, a so called "dissolvable" agent must be used on machines that are not under corporate administration.

11.1 Final thoughts

When starting this research project, I planned to test components with the open source network based NAC implementation Packetfence [17]. When I described the different stages of the architecture, I came to the conclusion that some more basic tests were needed. Although these tests were not conducted with Packetfence, the implementation supports or requires these techniques and the tests were therefore essential to conduct.
The infrastructure described in this document is deployable when there is no limit on physical resources (i.e. server hardware). VI's network is also present on temporary locations where only a connection to the head office is in place. A collapsed NAC design or usage of the central NAC infrastructure for these locations should be investigated.
In the end, I believe that with this report VI is able to verify which NAC products satisfy it's demands. Also, VI can improve current organizational processes to prepare them for NAC.

11.2 Future research

While performing this research, multiple questions remained unanswered due to the limited time:

- Monitoring and management demands on the solution are not described in this report. These demands should be investigated before the architecture is developed.
- Pre-admission evaluation on operating system and antivirus patch levels performs to slow through Nessus (7.4.6). It should be investi-

gated if this evaluation is possible through remote scripting and if this performs within the VI stated pre-admission time limit. (30 seconds)

- Effects on the described architecture when using VoIP devices and machines connected to these VoIP devices should be investigated.
- The implementation of the architecture on wireless networks should be investigated since the proposed techniques can be non applicable on such networks.
- One could issue that a NAC solution with user agents provides a better usability, because it is able to fix problems for the user. Maybe this is also possible by running specific remote scripts on affected hosts.

Other research questions are:

- Detection of the IDS system could be improved by implementing a honeynet.
- Inspection of traffic on Profinet by RT and IRT (2.4.1) could not be analyzed by Wireshark during tests, possibly because of their low latency. Analyses of inspecting this traffic requires attention when these networks must be protected by NAC.
- For VI, role based access in the production VLAN would be a logical next step after implementing NAC.

References

[1] *Vanderlande Industries Website*
http://www.vanderlande.com

[2] *Vanderlande Industries Annual Report 2008*
http://www.vanderlande.com/SiteCollectionDocuments/General/Annual_report_2008.pdf

[3] *Cisco Three Tier Network Model*
http://www.tech-faq.com/understanding-the-cisco/-three-layer-hierarchical-model.shtml

[4] *Wikipedia Profinet Article*
http://en.wikipedia.org/wiki/Profinet

[5] *Wikipedia Ladder Logic Article*
http://en.wikipedia.org/wiki/Ladder_logic

[6] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear
RFC 1918 Address Allocation for Private Internets, 1996
http://tools.ietf.org/html/rfc1918

[7] Ofir Arkin
Bypassing NAC v2.0, 2007
http://www.blackhat.com/presentations/bh-dc-07/Arkin/Presentation/bh-dc-07-Arkin-ppt-up.pdf

[8] *Wikipedia Ofir Arkin Article*
http://en.wikipedia.org/wiki/Ofir_Arkin

[9] Mike Fratto
Tutorial: Network Access Control (NAC), 2007
http://www.networkcomputing.com/showArticle.jhtml?articleID=201001835&pgno=1&queryText=

[10] *Trusted Computing Group*
https://www.trustedcomputinggroup.org/about/

[11] Richard Stallman
GNU Can You Trust Your Computer?, 2007
http://www.gnu.org/philosophy/can-you-trust.html

[12] *TCG Trusted Network Connect Architecture for Interoperability, 2005*
https://www.trustedcomputinggroup.org/groups/network/TNC_Architecture_v1_0_r4.pdf

[13] Jim Geier
Port Based Authentication Concepts, 2008
http://www.wireless-nets.com/resources/downloads/802.1x_book_c2.pdf

[14] *Wikipedia SNMP*
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[15] R. Frye, D. Levi, S. Routhier, B. Wijnen
RFC3584 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, 2003
http://tools.ietf.org/html/rfc3584

[16] *MAC Spoofing*
http://en.wikipedia.org/wiki/MAC_spoofing

[17] *PacketFence Administration Guide, 2008*
http://prdownloads.sourceforge.net/packetfence/PacketFence_Administration_Guide.pdf?download

[18] T. Bradley, C. Brown, A. Malis
RFC2390 Inverse Address Resolution Protocol, 1998
http://tools.ietf.org/html/rfc2390

[19] Andrew Dacey
How ARP Works
http://www.tildefrugal.net/tech/arp.php

[20] *ipNetToMediaTable SNMP Class*
http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.netcool_ssm.doc/rg/reference/appMIB2_ipNetToMediaTbl_r.html

[21] *What is port mirroring?, 2007*
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci511650,00.html#

[22] *Wireshark Website*
http://www.wireshark.org/

[23] *Wireshark Wikipedia Article Gratuitous ARP*
http://wiki.wireshark.org/Gratuitous_ARP

[24] *Microsoft Browser Announcements*
http://technet.microsoft.com/en-us/library/cc749904.aspx

[25] *How to Disable the Gratuitous ARP Function*
http://support.microsoft.com/kb/219374

[26] S. Cheshire, B. Aboba, E. Guttman
RFC3927: Dynamic Configuration of IPv4 Link-Local Addresses, 2005
http://www.faqs.org/rfcs/rfc3927.html

[27] Lars Strand
802.1X Port-Based Authentication HOWTO, 2004
http://tldp.org/HOWTO/html_single/8021X-HOWTO/#auth

[28] R. Housley, W. Ford, W. Polk, D. Solo
Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 1999
http://www.ietf.org/rfc/rfc2459.txt

[29] *Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows, 2003*
http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=05951071-6B20-4CEF-9939-47C397FFD3DD&displaylang=en

[30] T. Dierks, C. Allen
The TLS Protocol Version 1.0, 1999
http://www.ietf.org/rfc/rfc2246.txt

[31] *ProCurve Network Security solutions, The 802.1x solution*
http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm

[32] *Configuring IEEE 802.1x Port-Based Authentication*
http://www.ciscosystems.com/en/US/docs/ios/12_4t/12_4t11/ht_8021x.html

[33] David C. Plummer
An Ethernet Address Resolution Protocol, 1982
http://www.ietf.org/rfc/rfc826.txt

[34] *ARP Cache Poisoning*
http://www.grc.com/nat/arp.htm

[35] R. Droms
Dynamic Host Configuration Protocol, 1997
http://www.ietf.org/rfc/rfc2131.txt

[36] George Ou
An introduction to VLAN Trunking, 2003
http://www.lanarchitect.net/Articles/VLANTrunking/Introduction/

[37] *IEEE Std 802.1Q, 2005*
http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

[38] *Securing Networks with Private VLANs and VLAN Access Control Lists*
http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008013565f.shtml

[39] *Tenable Nessus*
http://www.nessus.org/nessus/

[40] *Common Vulnerabilities and Exposures Website*
http://cve.mitre.org/

[41] *Nessus Plugins Index*
http://www.nessus.org/plugins/index.php?view=all

[42] *Nessus Plugins SCADA*
http://www.nessus.org/products/professional-feed/index.php?view=scada

[43] *Snort Website*
http://www.snort.org

[44] Antonis Papadogiannakis, Demetres Antoniades, Michalis Polychronakis, and Evangelos P. Markatos
Improving the Performance of Passive Network Monitoring Applications using Locality Buffering
http://dcs.ics.forth.gr/Activities/papers/pcapLB-paper.pdf

[45] Petr Kobiersky, Jan Korenek
Traffic Scanner - Hardware accelerated IDS, 2007
http://tnc2007.terena.org/core/getfile.php?file_id=463

[46] David Davis
Limit bandwidth on a Cisco Catalyst switch port, 2008
http://www.zdnetasia.com/techguide/network/0,3800010800,62036059,00.htm

[47] *Chapter 2: Writing Snort Rules Tables 2.2, 2.3 and 2.4*
http://www.snort.org/docs/writing_rules/chap2.html#SnortDefaultClassifications

[48] Brian Laing
Internet Security System: How to guide (IDS), 2000
http://www.snort.org/docs/iss-placement.pdf

[49] Martin Roesch, Chris Green, Sourcefire Inc.
Snort Users Manual, 2.6.1
http://www.snort.org/docs/snort_htmanuals/htmanual_261/snort_manual.html

[50] *McAfee Stinger Website*
http://vil.nai.com/vil/stinger/

[51] *NessusClient 3.2 User Guide, 2008*
http://www.nessus.org/documentation/NessusClient_3.2_User_Guide.pdf

[52] *Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module*
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html

Appendix A: Endpoint Security Threats

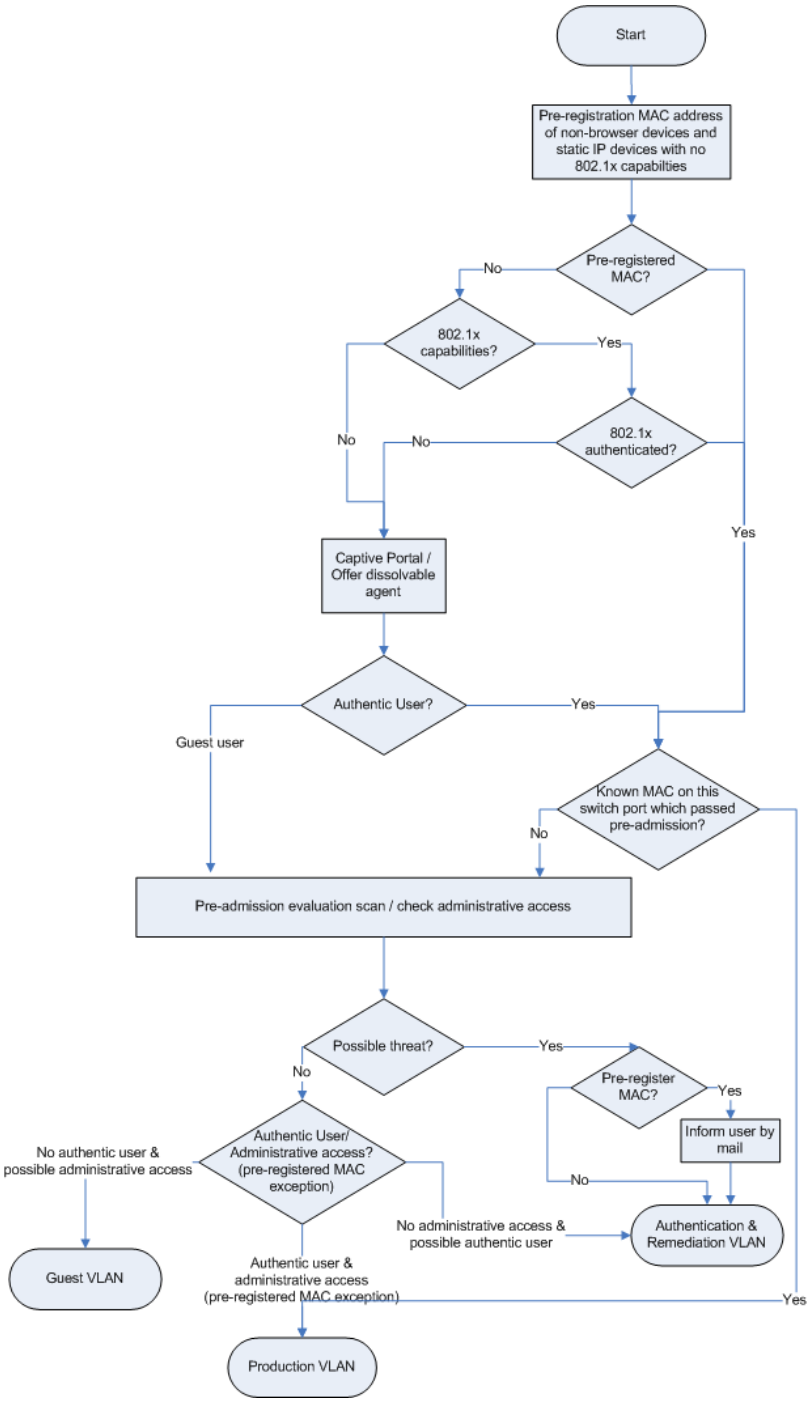
The following information is based on IT Questionnaire conducted during the research. The threat mapping is based on the categories plug-ins available for Nessus [39] the number 1 vulnerability scanner according to sectools.org.

Type of system	Workstation/server system
Operating system type	Microsoft Windows Based
Currently used in organisation	Windows XP, Windows 2003
Known threats	application/service exploits, backdoors, database exploits, denial of service, finger abuse, firewall attacks, FTP attacks, open system (shares), operating system (patches), RPC, shell access exploits, SMTP issues, SNMP issues, bad user management or default account misuse, virusinfections, web server attacks

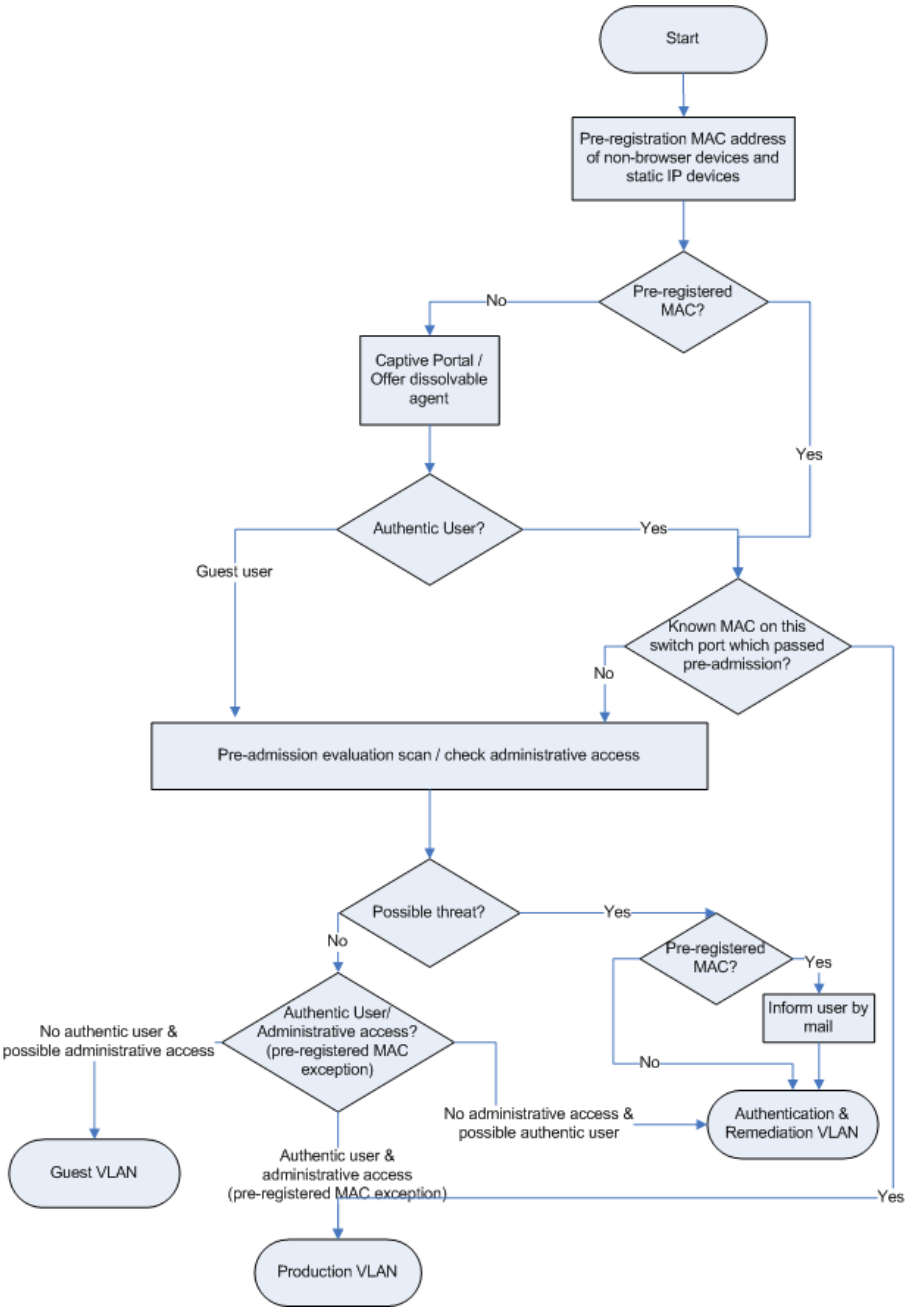
Type of system	Flow System Controller (FSC) Industrial PC hardware (x86 oriented)
Operating system type	Unix Based
Currently used in organisation	QNX
Known threats	application/service exploits, backdoors, database exploits, denial of service, finger abuse, firewall attacks, FTP attacks, open system (shares), operating system (patches), RPC, security shell access, SMTP issues, SNMP issues, bad user management or default account misuse, web server attacks

Type of system	SCADA Programmable Logic Controller (PLC)
Operating system type	None, setup is hard coded
Currently used in organisation	Siemens 300/400 series
Known threats	application/service exploits, backdoors, denial of service, finger abuse, FTP attacks, security shell access, SNMP issues, bad user management or default account misuse, web server attacks (when available)

Appendix B: 802.1x Flowchart



Appendix C: Captive Portal Flowchart



Appendix D: Snort Rules

snort.conf

```
#=========================================
# Include all relevant rulesets here
#
# The following rulesets are disabled by default:
#
#   web-attacks, backdoor, shellcode, policy, porn, info, icmp-info,
#   virus, chat, multimedia, and p2p
#
# These rules are either site policy specific or require tuning in order
# to not generate false positive alerts in most environments.
#
# Please read the specific include file for more information and
# README.alert_order for how rule ordering affects how alerts are
# triggered.
#=========================================

include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
# include $RULE_PATH/scan.rules
# include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
# include $RULE_PATH/tftp.rules

include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-php.rules

include $RULE_PATH/sql.rules
include $RULE_PATH/x11.rules
# include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/oracle.rules
include $RULE_PATH/mysql.rules
# include $RULE_PATH/snmp.rules

include $RULE_PATH/smtp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/pop2.rules
include $RULE_PATH/pop3.rules

include $RULE_PATH/nntp.rules
# include $RULE_PATH/other-ids.rules
# include $RULE_PATH/web-attacks.rules
include $RULE_PATH/backdoor.rules
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
```

```
# include $RULE_PATH/porn.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/p2p.rules
include $RULE_PATH/spyware-put.rules
include $RULE_PATH/specific-threats.rules
# include $RULE_PATH/experimental.rules
# include $RULE_PATH/content-replace.rules
include $RULE_PATH/voip.rules
```

Appendix E: Environments Overview