

Bypassing NAC v2.0

Ofir Arkin, CTO

BlackHat DC 2007

ofir.arkin@insightix.com
<http://www.insightix.com>



Updated Presentation

Download from:

http://www.sys-security.com/OA_Bypassing_NAC_DC_07.ppt.zip [~1.5mb]

What this talk is about?

- Introduction to NAC
 - What is NAC?
 - What problem does NAC aim to solve?
 - A NAC solution's components
- Bypassing NAC
 - Architecture
 - Element Detection
 - Compliance Checks
 - Enforcement
 - Quarantine
 - Etc.
- Product Examples

Ofir Arkin

- CTO and Co-Founder, Insightix
<http://www.insightix.com>
- Founder, The Sys-Security Group
<http://www.sys-security.com> (Blog)
- Computer Security Researcher
 - Infrastructure Discovery
 - ICMP Usage in Scanning
 - Xprobe2 (The Active OS Fingerprinting Tool)
 - Risks of Passive Network Discovery
 - VoIP Security
 - Information Warfare
 - NAC
- Member
 - VoIPSA (Board member, Chair security research committee)

Introduction

Introduction

What is NAC?

- Truths about NAC:
 - A hot topic
 - The Next Big Thing in the IT security space
 - A misused term used by some vendors to get visibility
 - A bandwagon a lot of companies wants to jump on
 - Many products available today claiming to offer NAC
 - A misconception created due to lack of standardization and a common definition
 - The first concept introduced (2003) by Cisco as a means to combat viruses and worms as a lesson from Blaster

Introduction

What is NAC?

- What exactly is NAC?
 - A compliance solution?
 - A security solution?
- What problem does it aim to solve?

Introduction

The Problem

- An enterprise IT network is a **complex** and a **dynamic** environment that is generally described as a **black hole** by its **IT managers**
- The **lack of knowledge** results in **lack of control**, the **inability** to **manage** and **secure** the enterprise IT network in an appropriate manner
- The **stability**, **integrity** (viruses, worms, information theft, etc.) and **regular operation** of the IT network are in **jeopardy** due to the **lack of knowledge** regarding the enterprise **network layout** (topology), **resources** (availability and usage), **elements residing on the network** (devices, applications, their properties and the interdependencies among them) and **users** accessing the network and their resources (whether locally or remotely)

Introduction

The Problem

- The threat of **viruses, worms, information theft, roaming users**, and the **lack of control** of the IT infrastructure lead companies to seek security solutions which **control the access to their internal IT networks**
- A new breed of software and hardware solutions from a variety of vendors has recently emerged
- All are tasked with one goal – **controlling the access to a network** using **different methods and solutions**

Introduction

My NAC is not Your NAC

- **Standardization** and/or a **common criterion** for NAC **does not exist**
 - Cisco **N**etwork **A**dmission **C**ontrol (NAC)
 - Microsoft **N**etwork **A**ccess **P**rotection (NAP)
 - The **T**rusted **C**omputing **G**roup (TCG), **T**rusted **N**etwork **C**onnect (TNC)
 - Etc.
- Therefore 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**

Introduction

What NAC Is

- The basic task of NAC is to **control access**
- The secondary task of NAC is to **ensure compliance**
- As such NAC is **first and foremost** a security solution and **only then** a compliance solution
- NAC is a **risk mitigation security solution**
- My definition of NAC is:
 - **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

Capabilities

Capabilities

The Basics

- The most essential capabilities any NAC solution must have are the ability to **detect a new element connecting to the network**, and the ability to verify whether or not it **complies** with a defined security policy
- If the element is not authorized and/or does not comply with the defined security policy, the NAC solution must **restrict** the element's **access to the network**

Capabilities

NAC Functions

- The following is a list of functions a NAC solution **may**, or **may not** support
 - **Element detection** – The ability to detect new elements as they are introduced to the network
 - **Authentication** – The ability to authenticate each user accessing the network no matter where they are authenticating from and/or which device they are using

Capabilities

NAC Functions

- **End point security/compliance assessment** – The ability to **assess** whether a **newly** introduced network element **complies** with a defined **security policy**. These checks may include the ability to **gather knowledge** regarding an element's **operating system**, the list of **installed patches**, the presence of an **A/V software** (present, running, and updated), **installed applications**, etc.
- **Quarantine** – The process of **isolating** an **element** from the rest of the network. Quarantine can be triggered when **a new element is detected to operate on the network** and/or when **an element is non-compliant with the defined security policy**. When quarantined, the element should be able to **access** a defined set of **remediation servers** allowing the user fixing the non-compliant issues

Capabilities

NAC Functions

- **Remediation** – The process of fixing an issue causing an element to be non-compliant with the defined security policy
- **Enforcement** – Is the process of **restricting** the element's **access** to the network if found to be **non-compliant with the defined security policy**
- **Authorization*** - The ability to **verify access** by users **to network resources** **complies** with an **authorization scheme** defined in an existing authorization system (such as Active Directory, RADIUS servers, etc.) allowing enforcing identity-based policies

Capabilities

NAC Functions

- **Post-Admission Protection** – Is the process of **continuously monitoring** users, elements and their actions for **suspicious activity** (i.e. spoofing, worms, viruses, malware, etc.). If detected the action taken by a NAC system may vary from isolating the offending system to dropping the session

NAC Functions

A Few Remarks

- Functionality which may not belong under the NAC hat:
 - Authorization
 - “Who access which resource” is something which should be defined by the business people of an organization
 - Specialized technologies are designed to enforce authorization rights in the IT environment
 - Microsoft Windows Domain hierarchy
 - Single sign-on
 - Firewalls
 - Etc.
 - Post-Admission protection
 - Abnormality detection companies which jumps the bandwagon of NAC
 - Dumb down/‘Simplified’ solutions (i.e. IP addresses which does not exist, etc.)

Attack Vectors

Attack Vectors

- A solution's architecture
 - The placement of the different pieces of a solution
- Technology used
 - Element detection
 - Quarantine abilities
 - Enforcement methods
 - End-point security assessment
 - Etc.
- A solution's components
 - Client-side software
 - Server-side software (and hardware)

Bypassing NAC Background

Technology Used

Bypassing

Element Detection

- Element detection is a **core feature** that **must** be supported by **any** NAC solution
- Way of operation
 - **Element detection** provides the ability to detect a new element operating on the network
 - **Element detection** must detect, in real-time, a new element as it attempts to attach itself to the network
- **!** If a NAC solution cannot perform element detection in real-time then it **does not provide a valuable line of defense**
- It is simply because you cannot expect a NAC solution to **defend against devices it is not aware of**

Element Detection

Questions to Ask

- How does the NAC solution detects the presence of a new element?
- Does element detection performed in real-time?
- How does the information regarding the elements residing on the network stays current?

Element Detection

Methods

- DHCP proxy
- Authenticated DHCP (NAC-in-a-Box)
- Broadcast listeners
- Switch integration
- 802.1x
- Agent software
- In-line devices
- Out-of-band devices
- Proprietary methods

Basics

Quarantine

- There are a **variety** of quarantine **methods** available, each with varying **strengths** and **weaknesses**
- The quarantine holds '**soft targets**' that can be **easily attacked** and **penetrated** into
 - There is a reason why an element is in quarantine...
 - Does not comply with the security policy (patch, A/V, etc.)
 - The level of security of these elements will be the lowest of all elements residing on the network
- **!** It is important to understand whether a quarantine method a certain NAC solution uses can be **bypassed**
- **!** Another key point is whether a quarantine method a certain NAC solution uses may allow a quarantined element to **interact** with **other quarantined elements**

Basics

Quarantine

- If the quarantine area is **a shared medium** (i.e. separate Subnet/VLAN) between the quarantined elements they might be able to **infect** and/or **penetrate** each other
- In case it is a shared medium the quarantine area makes the **perfect attack vector**
 - An attacker connects its machine to the network
 - The attacker's machine will be quarantined
 - The attacker may access any element on the quarantine
 - Infection
 - Control

Quarantine

Questions to Ask

- How does the quarantine mechanism **operates**?
- Is the quarantine area a **shared medium**?
- Can the quarantine method **isolate** an element **as soon as** it tries to attach itself to the network?
 - Blocking possible interaction with other elements on the network until the state of the questionable element is determined
 - Does this mandates using the switch (i.e. relying on the switch abilities)?
- Does the quarantine method rely on specialized hardware or software?
- Does the quarantine method rely on **switch integration**?
 - Separate VLAN: Where is the VLAN termination?
- Can the quarantine mechanism quarantine **virtual machines**
 - Virtualization becomes an integral part of the data center (as well as QA and R&D environments)

Quarantine

Needed Solution

- Use a quarantine method able to provide with a **private quarantine**
 - **Shielding** the quarantined element from the **network** and from **other quarantined elements**
- Quarantine a device into a private VLAN (PVLAN) with no access to other elements on the network (except for remediation servers)

Basics

Enforcement

- How is enforcement performed?
- Is the enforcement performed at L2 or at L3?
 - L3: **Bypassable**, creates isolated shared islands (subnets)
 - L2: Most powerful, usually done with manipulating ARP tables. **In many situations it can be bypassed**. Its power depends on the technique used.
- Does the enforcement involves the networking gear?
 - I.E. Cisco, Juniper, Extreme, etc. (where strength vary according to the switch manufacture)
 - Must be **one vendor shop**
- Does the enforcement depends on **specialized software**?
 - I.E. Agent software
- Does enforcement operates against all OSs?
- Does the enforcement depends on **specialized hardware**?
- Is the NAC solution capable of enforcing the NAC policy against individual virtual machines?

Enforcement

Methods

- Switch integration
 - 802.1x
 - Shutting down switch ports
 - Assigning separate VLANs
- DHCP
 - Separate subnet
- IPS style shootem' up
- Layer 2
 - Manipulating ARP tables
- In-Line devices
- Etc.

End-point Compliance Assessment

- End point compliance checks are designed for **risk reduction** (and compliance)
- What is the list of parameters that can be checked when an element is being admitted to the network?
- Potential Issues
 - Agent-based Vs. Agent less
 - Managed Vs. Unmanaged elements
 - Microsoft Windows vs. Other operating systems

End Point Compliance Assessment

Agent-based

- Strengths
 - Provides a wealth of information regarding a host and its known security state (OS, patches, A/V Signatures)
 - May detect changes

End Point Compliance Assessment

Agent-based

■ Weaknesses

- Where to install the clients?
- Another client among many
- May have a performance impact against the element
- Usually available for Microsoft Windows operating systems only
- Management overhead (can be a nightmare)
- Takes time to implement
- Security issues with the client software
 - Attacks directed at the client
 - Bypassing the client enforcement
 - Right-click to disable (Symantec, fixed)
 - Cisco
- The information which needs to be extracted from the elements may be easily spoofed (For example, Windows OS version, Service Pack version installed, patches installed, etc.)

End Point Compliance Assessment

Agent-based

- Weaknesses (cont.)
 - **Unmanaged** elements
 - Problem I: Knowing they are out there
 - Problem II: External vulnerability scans (a big duh!)
 - Problem III: Dissolving agents
 - **No custom checks**, limited to a pre-defined set of checks

End Point Compliance Assessment

Agent-less

■ Strengths

- No need to install additional software
- Fast deployment
- Introducing custom checks is easier

■ Weaknesses

- Information regarding a certain element may not always be available (i.e. service not available, unmanaged device, device property which cannot be reported through a management service, etc.)
- Less granular information
- The information which needs to be extracted from the elements **may be easily spoofed** (For example, Windows OS version, Service Pack version installed, patches installed, etc.)

End Point Compliance Assessment Dissolving Agent

- Weaknesses
 - Usually available for Microsoft operating systems (i.e. Active-X control)
 - Requires local administrator rights or power user rights
 - In enterprise environments users may have limited local rights

End Point Compliance Assessment

The Real Risk

- It all breaks down to what is being checked, and does the information is helpful or not
 - Patches
 - Security related patches (and other patches) are **not enrolled** into the enterprise **as soon as they are available**
 - It may take **months** to **enroll a major security update** of an operating system (i.e. Microsoft Windows XP SP2, Microsoft Windows 2003 SP1)
 - Zero day is not blocked
 - The checks performed may be useless against 0-day attacks
 - Zero day viruses, worms, and vulnerabilities **may not be detected**, and remediation will not be available
 - Understanding the real risk
 - The risk from an element does not only rely on the version of the A/V signature file it may be running (I.e. information theft, unauthorized access, etc.)
- End point compliance checks are designed for risk reduction
- Risk mitigation is a key in reducing the overall security risk an enterprise is facing

Bypassing NAC Background

Solution Components

Solution Components

Software Clients

- “There is no such thing as client-side security”
- <http://www.cisco.com/warp/public/707/cisco-sa-20070221-suplicant.shtml>
 - Cisco Security Advisory: Multiple Vulnerabilities in 802.1X Suplicant

Bypassing NAC Examples

Examples

- DHCP Proxy
- Authenticated DHCP / DHCP in-a-box
- Broadcast Listeners
- Switch Integration
- 802.1x
- Cisco NAC Framework
- In-Line devices
- Out-of-Band devices

Bypassing NAC

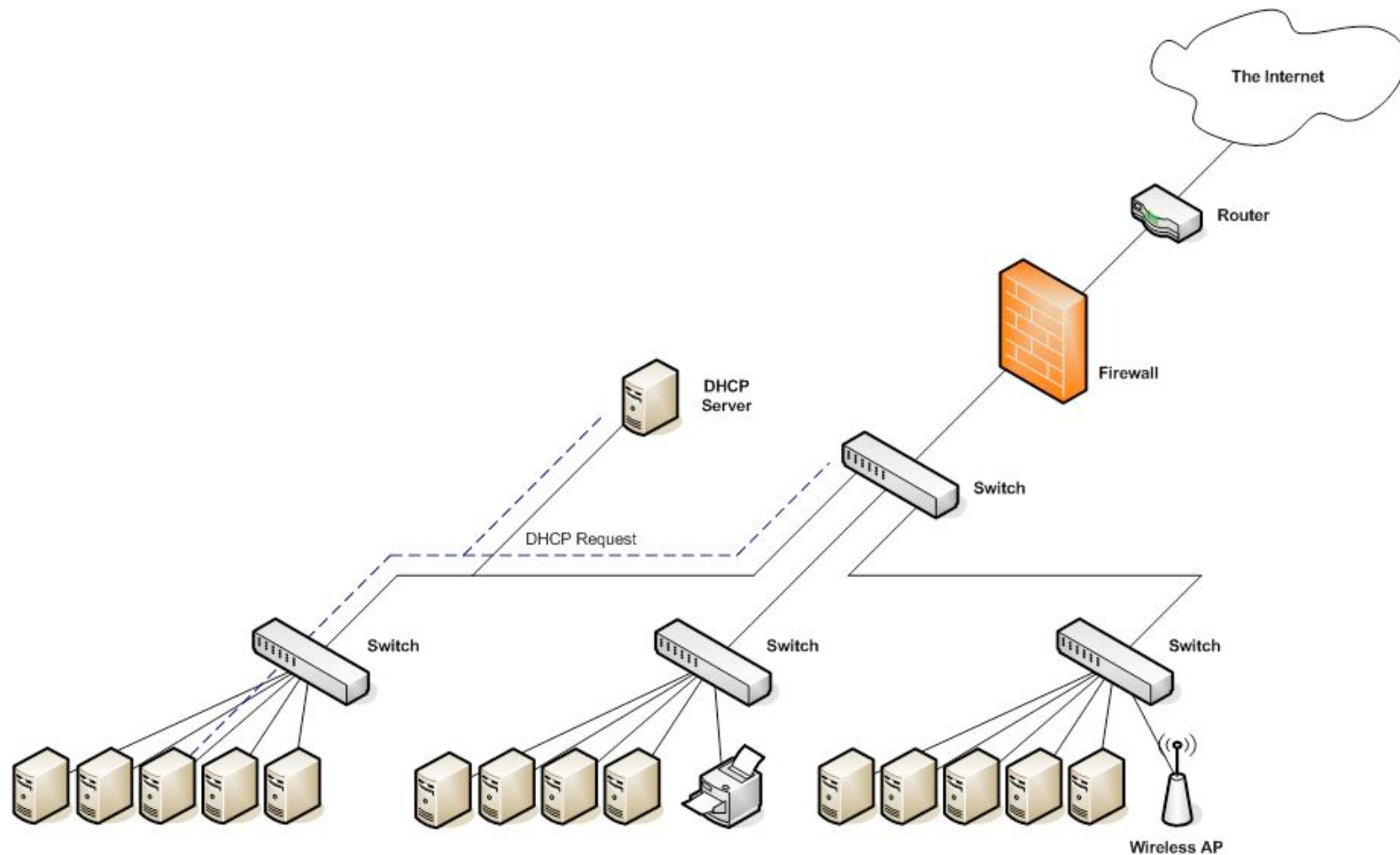
Examples

- The examples following were taken from different vendor offerings
- There may be other combinations/offerings which are not covered in this presentation
- The information provided would allow to figure out their issues

DHCP Proxy

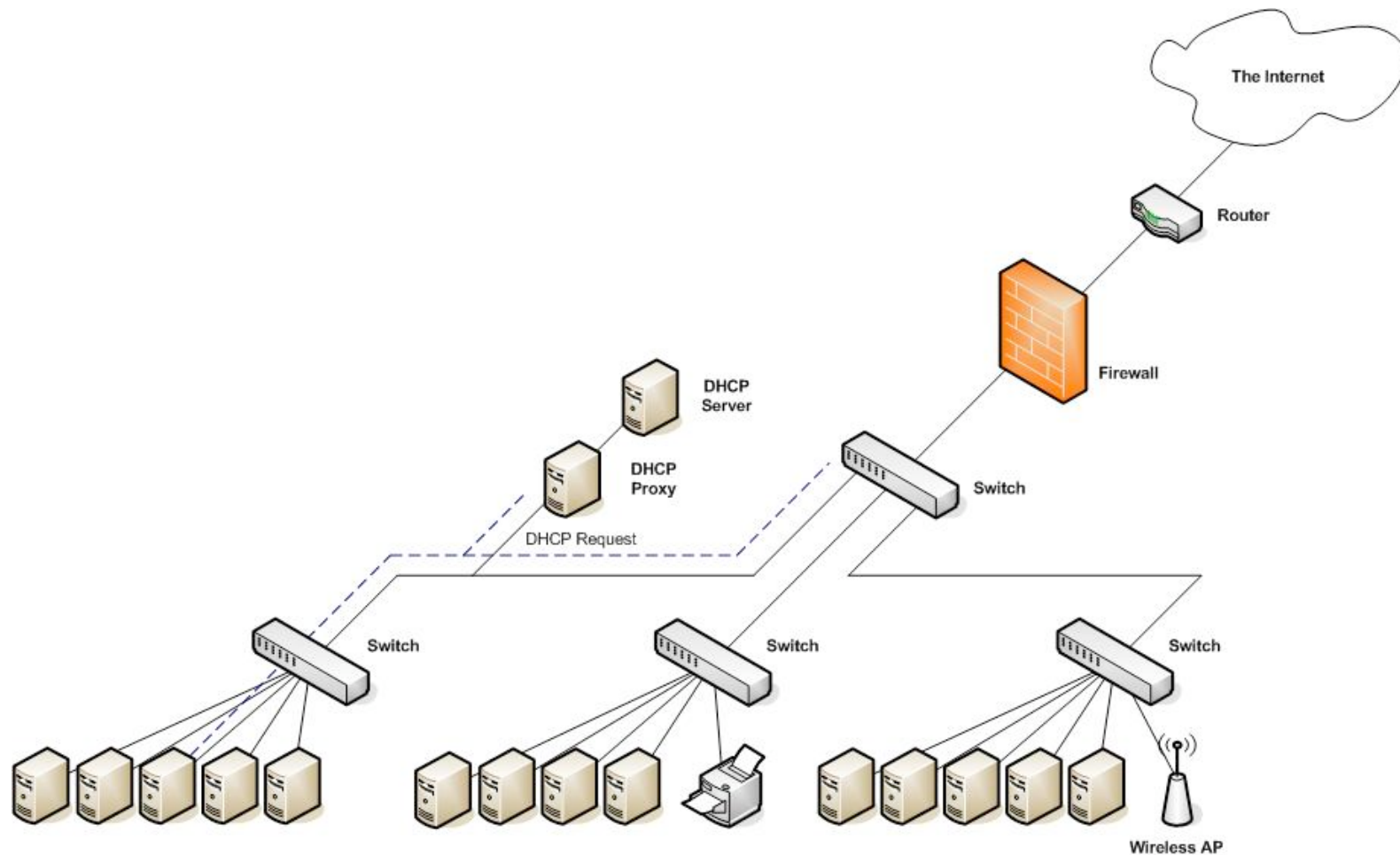
DHCP Proxy

Architecture



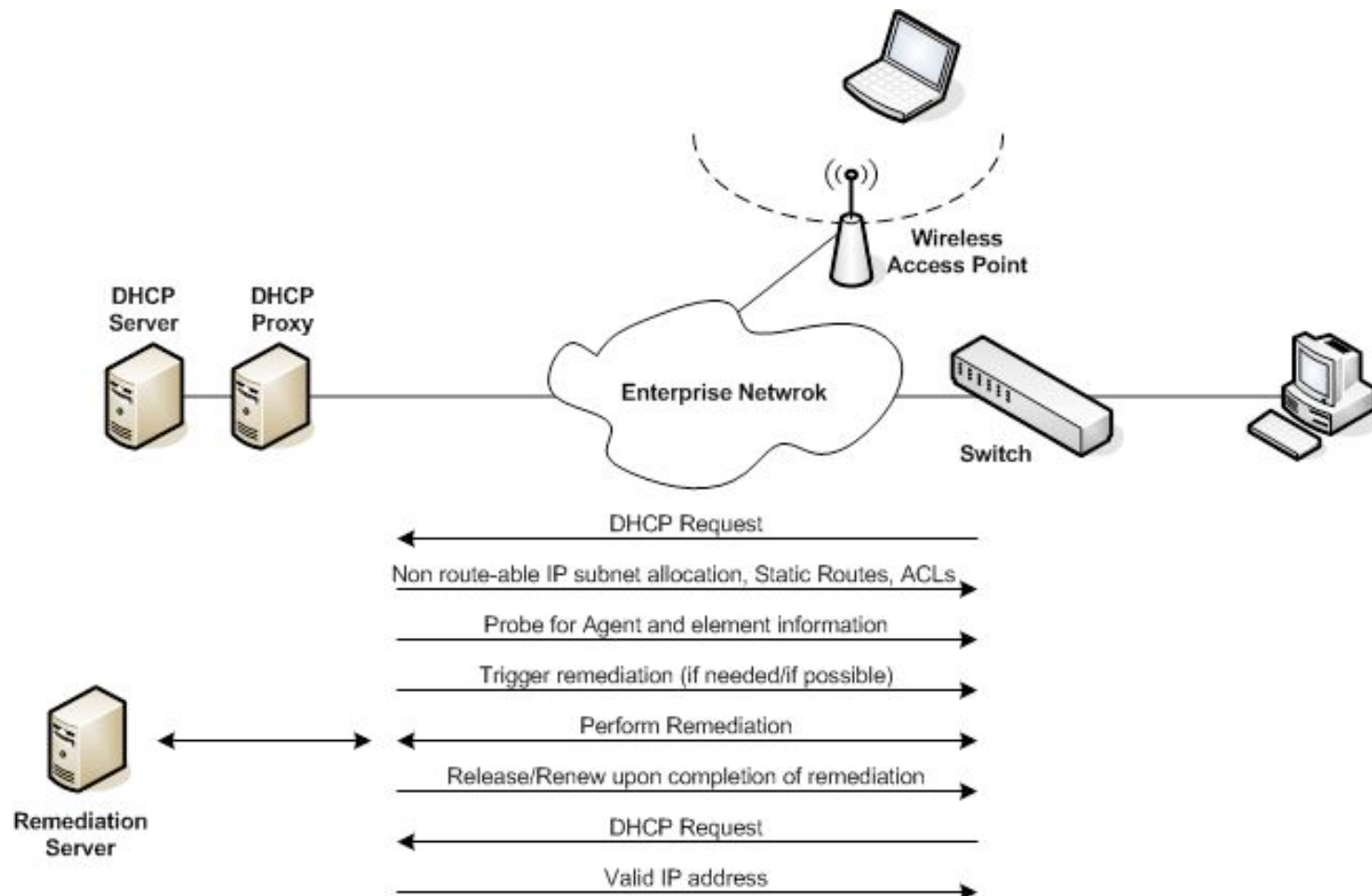
DHCP Proxy

Architecture



DHCP Proxy

Information Exchange



DHCP Proxy

Strengths

- Most organizations use DHCP
- Easy to deploy
- Fast to deploy

DHCP Proxy

Weaknesses

- Detected elements are **only those using DHCP**
 - Not all of the elements residing on the enterprise network will be using DHCP (I.e. Servers, Printers, etc.)
 - **Incomplete detection** of elements operating on the network. **Other** elements may exist and operate on the network
 - **Bypassing** DHCP Proxy NAC by simply assigning **a static IP address** for an element
- Elements **must use agent software** with this type of solution
 - Usually available for Microsoft Windows-based OSs only
 - Without the usage of agent-based software there is an **inability to determine** whether an element comply, or not, with the enterprise security policy
- **Detection** of elements is done at **Layer 3** only
 - An element can connect to the network **without being detected**
 - **Access** to at least the local subnet will **not be restricted**

DHCP Proxy

Weaknesses

- **Enforcement** is performed **at Layer 3** only
 - The local subnet is a shared medium
 - Elements can **infect** and/or **penetrate** other elements on their subnet, and cannot be stopped
 - Bypassing enforcement by attacking a system on the local subnet using it as an '**access proxy**' to other parts of the enterprise network
- Quarantine of an element is done using non-routable IP addresses and ACLs on routers (Layer 3 only)
 - **Bypassing** the quarantine by assigning an element a static IP address
 - The local subnet is a shared medium
- No actual knowledge regarding what is on the enterprise network?
 - No actual knowledge of what is on the network
 - No knowledge on the actual network topology may lead the existence of other, **uncovered venues** to access the network

DHCP Proxy

Weaknesses

- Not able to detect masquerading elements hiding behind an allowed elements (i.e. **NAT**)
 - Virtualization as a major issue (i.e. Freebee virtualization software such as Virtual PC, Vmware, etc.)
- Exceptions needs to be manually inputted (i.e. printers)
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address and/or the IP address of an exception in order to receive full access to the enterprise network
- Cannot be extended to include remote users
- There is no form of **user authentication** (i.e. theoretically, install an appropriate client, be compliant with the security policy, access is granted)

DHCP Proxy

Weaknesses

- The problem of unmanaged elements
 - “Systems without agents can be granted network access two ways. First, a **non-windows exception can be made that exempts non-windows clients from the NAC process.** Second, **a MAC address-based exemption list can be built.** This MAC address list accepts wildcards, allowing the exemption of whole classes of systems such as IP phones using their Organizationally Unique Identifiers.”
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address and the IP address of an exception in order to receive full access to the enterprise network

Source: “Network Access Control Technologies and Sygate Compliance on Contact”, Sygate/Symantec

DHCP Proxy

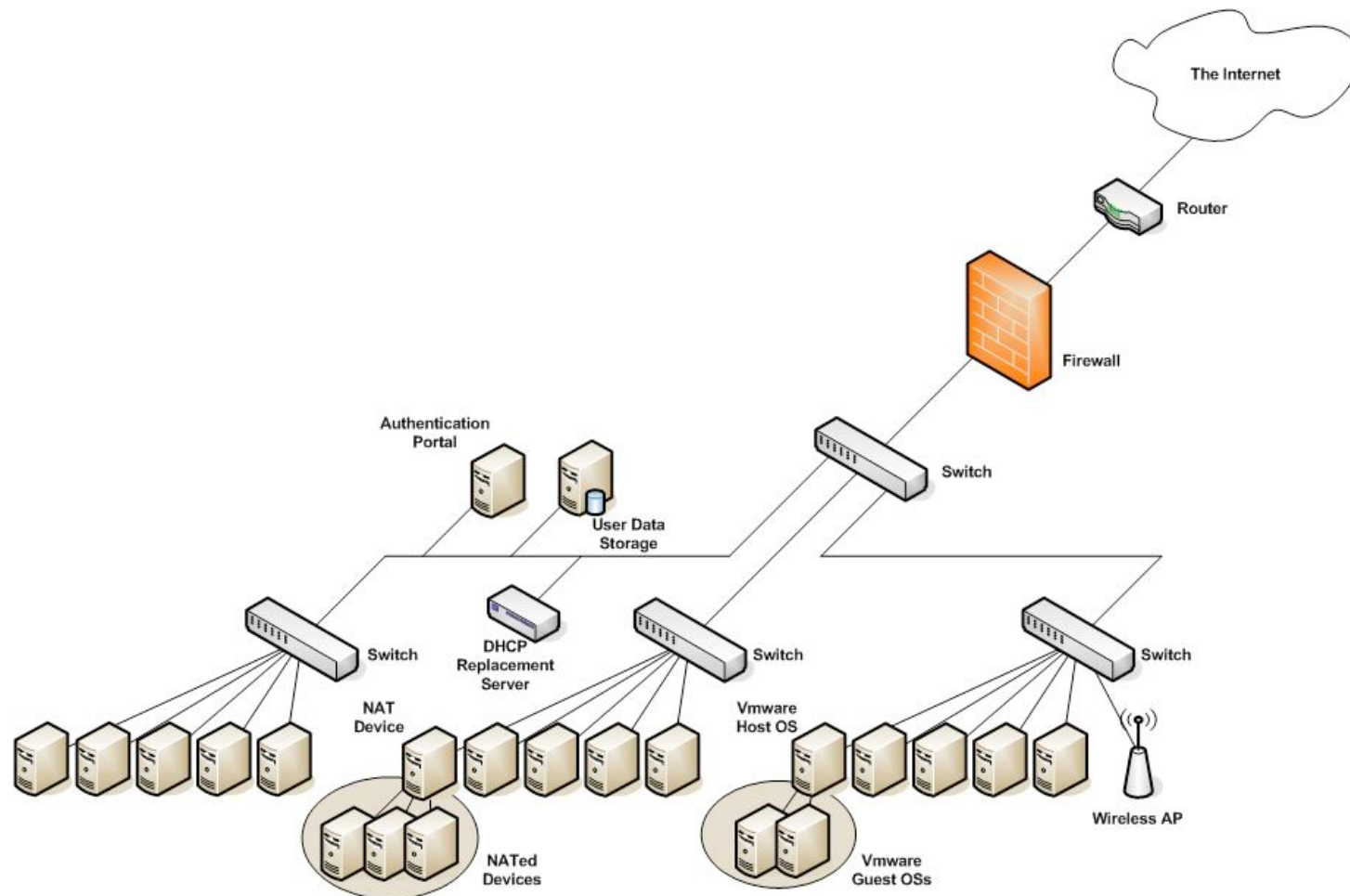
Solutions Supporting DHCP

- Like in Blackjack: Too many

Authenticated DHCP or DHCP In-a-Box

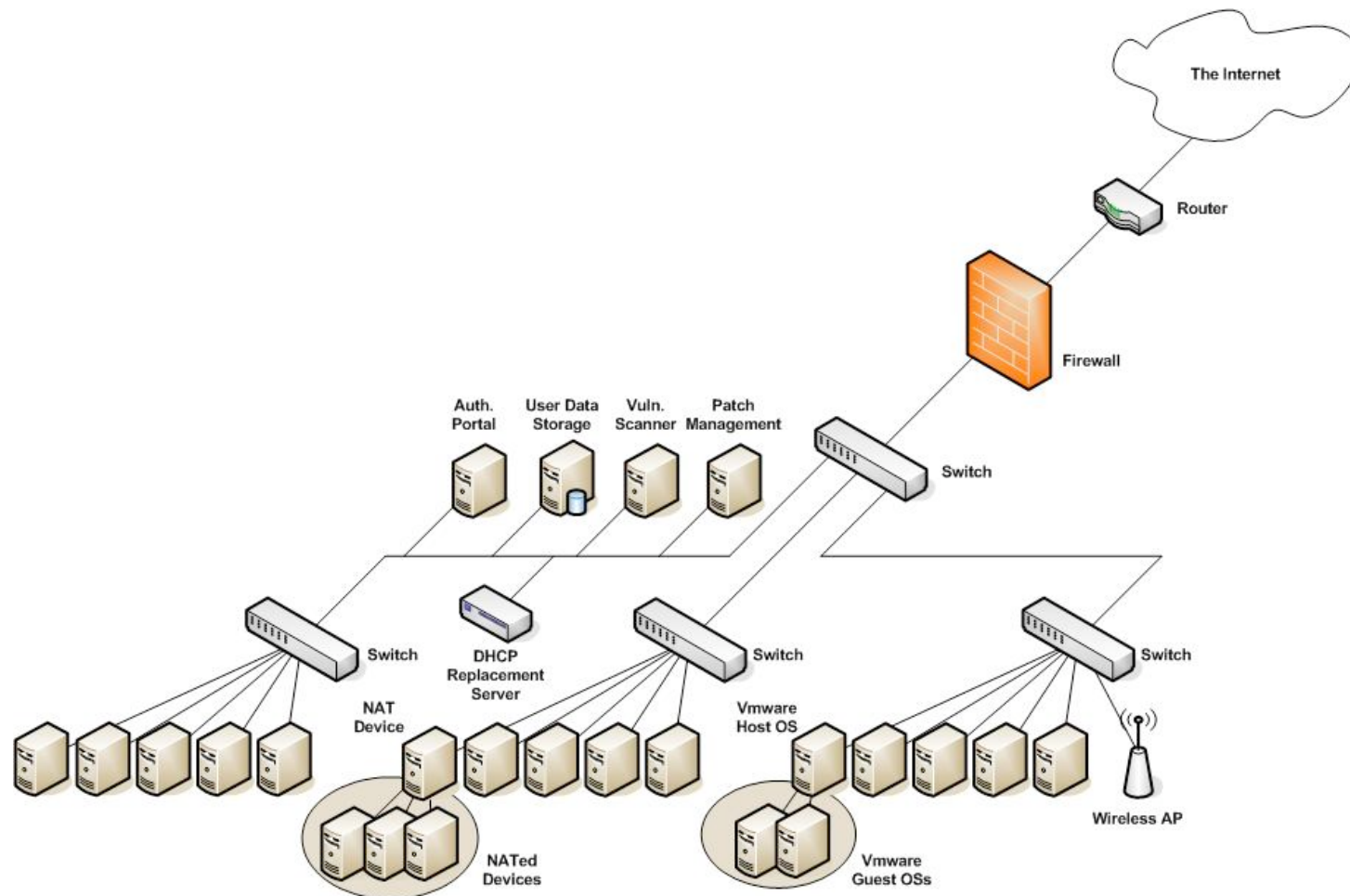
DHCP In-A-Box

Architecture



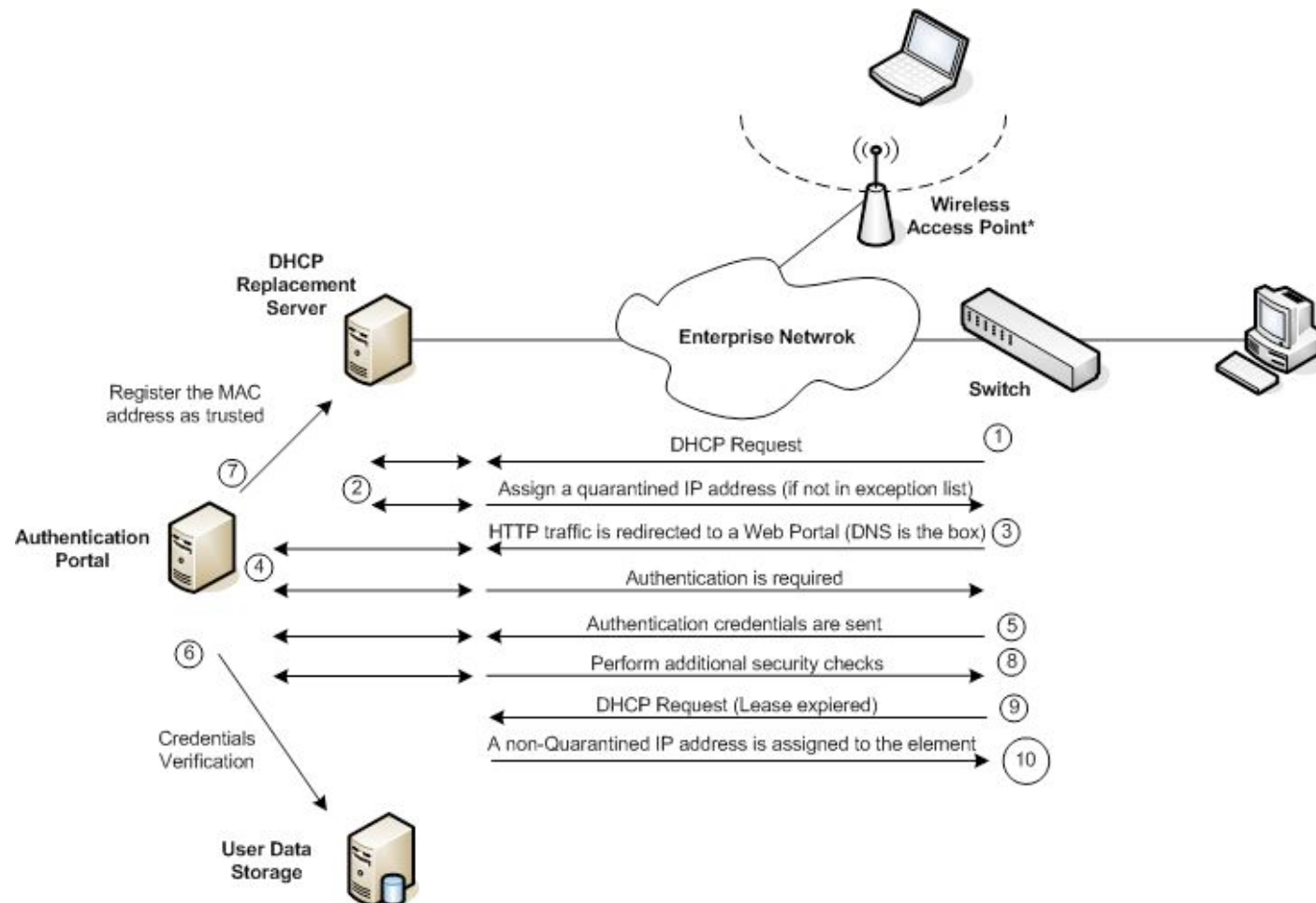
DHCP In-A-Box

Architecture



DHCP In-A-Box

Information Exchange



DHCP In-A-Box

Strengths

- Theoretically, may authenticate any user trying to access the network
- Theoretically, operating system independent
- Most organizations use DHCP
- Easy to deploy
- Fast to deploy

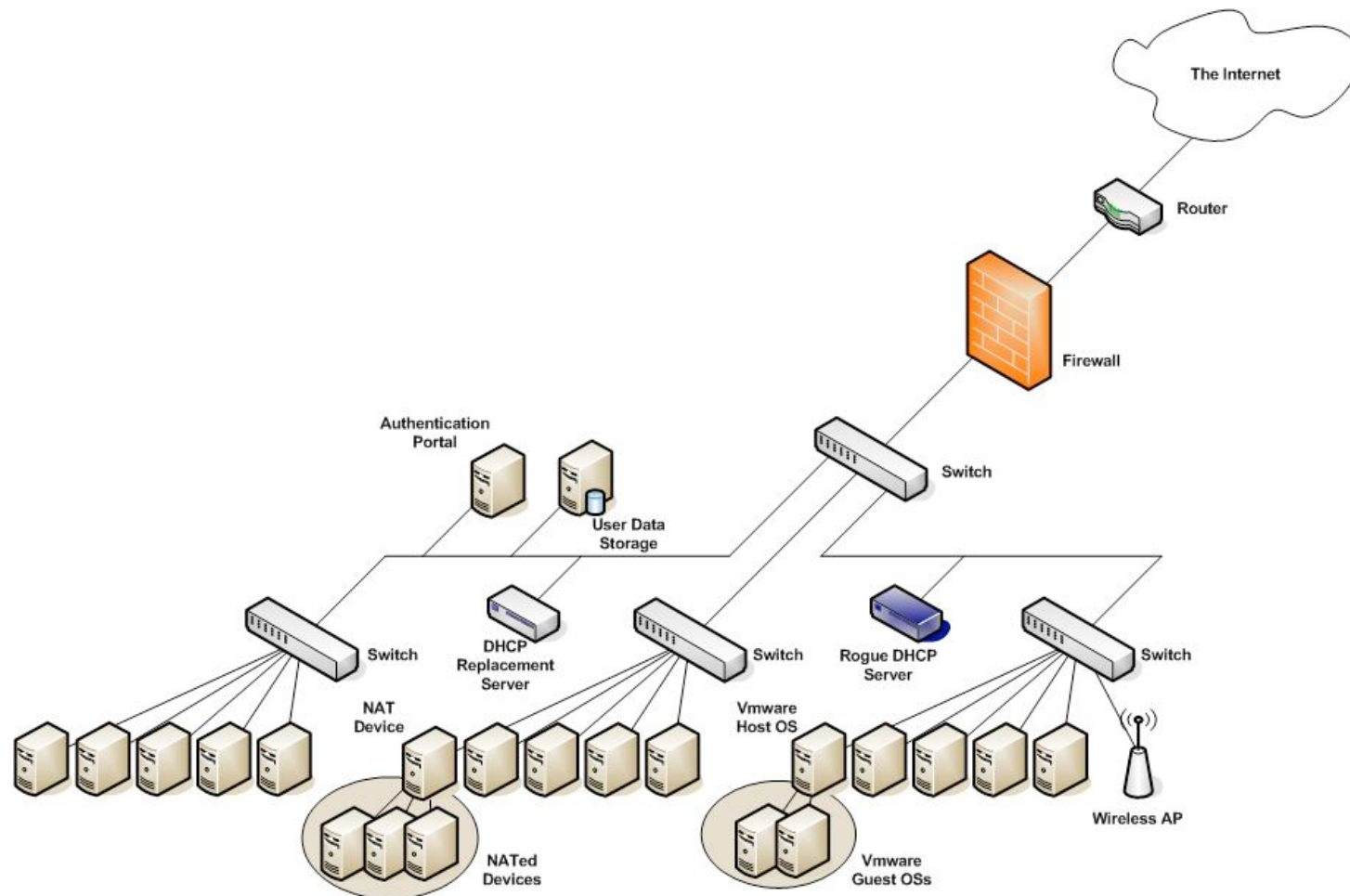
DHCP In-A-Box

Weaknesses (Highlights)

- Detected elements are **only those using DHCP**
- Detection of elements at **Layer 3** only
- **Enforcement** is performed at **Layer 3** only
- No knowledge of the who is on the network
- There is **no knowledge** about the **exception elements**
- Uses 3rd party products to asset the security of elements
 - No real-time assessment
 - In some cases, these checks would prove useless (I.e. FWed elements, etc.)
- All other DHCP Proxy weaknesses apply

DHCP In-A-Box

Rogue DHCP Server



DHCP In-A-Box

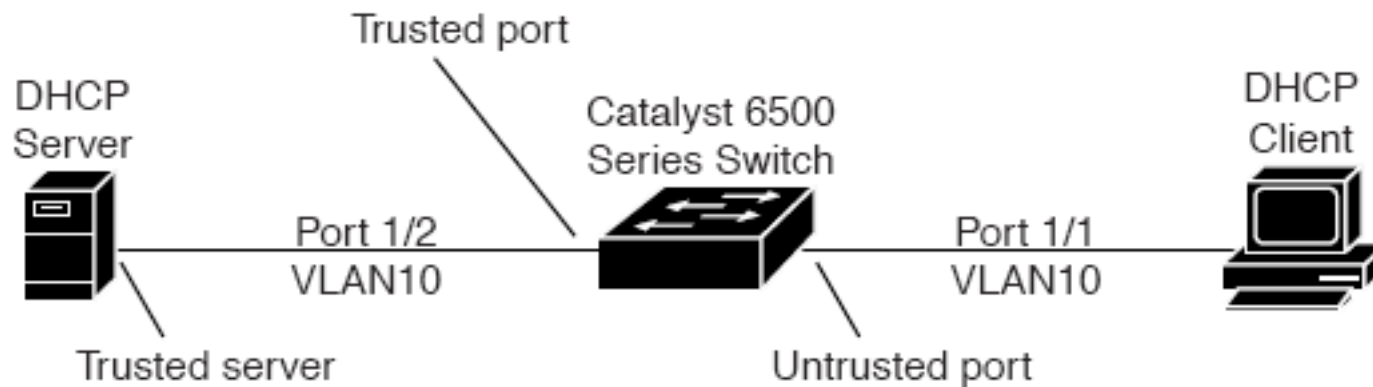
Rogue DHCP Server

- The first DHCP server's reply to reach a host sending a DHCP request would assign the DHCP server responding to be used by the element
 - Assign the element a “quarantined” IP address
 - Direct DNS traffic to the rogue DHCP Server by assigning the DNS server's IP address with the DHCP reply to the rogue DHCP server
 - Present the user with a look-a-like authentication page (using HTTPS, preferred)
 - Abuse the credentials collected
 - For example, wait for the disconnection of the element and abuse its credentials
 - Etc.

DHCP NAC

The Switch Manufacture Case

DHCP NAC Switch Manufacture Architecture



DHCP NAC Switch Manufacture

Weaknesses

- The **policy is defined per-port**, so it should be configured... per-port
- **Not all** the elements on the network are **using DHCP**
- It is a **must prior to deployment** to fully **map the environment** understanding **which elements are connected where**. This is done in order to understand what policy should be defined against which switch ports
- Enforcing policy (via ACLs) against rogue DHCP servers must be done **across the entire enterprise** (all switches) to make sure there are no venues of bypassing this enforcement
 - This suggest the enterprise should have networking gear from the same manufacture
- Large enterprises == a big management headache
- Connecting devices would now be according to which switch ports they can connect to. This is a **management nightmare** in a large organization.
- Enforcement is done **per port per a single element**

DHCP NAC Switch Manufacture

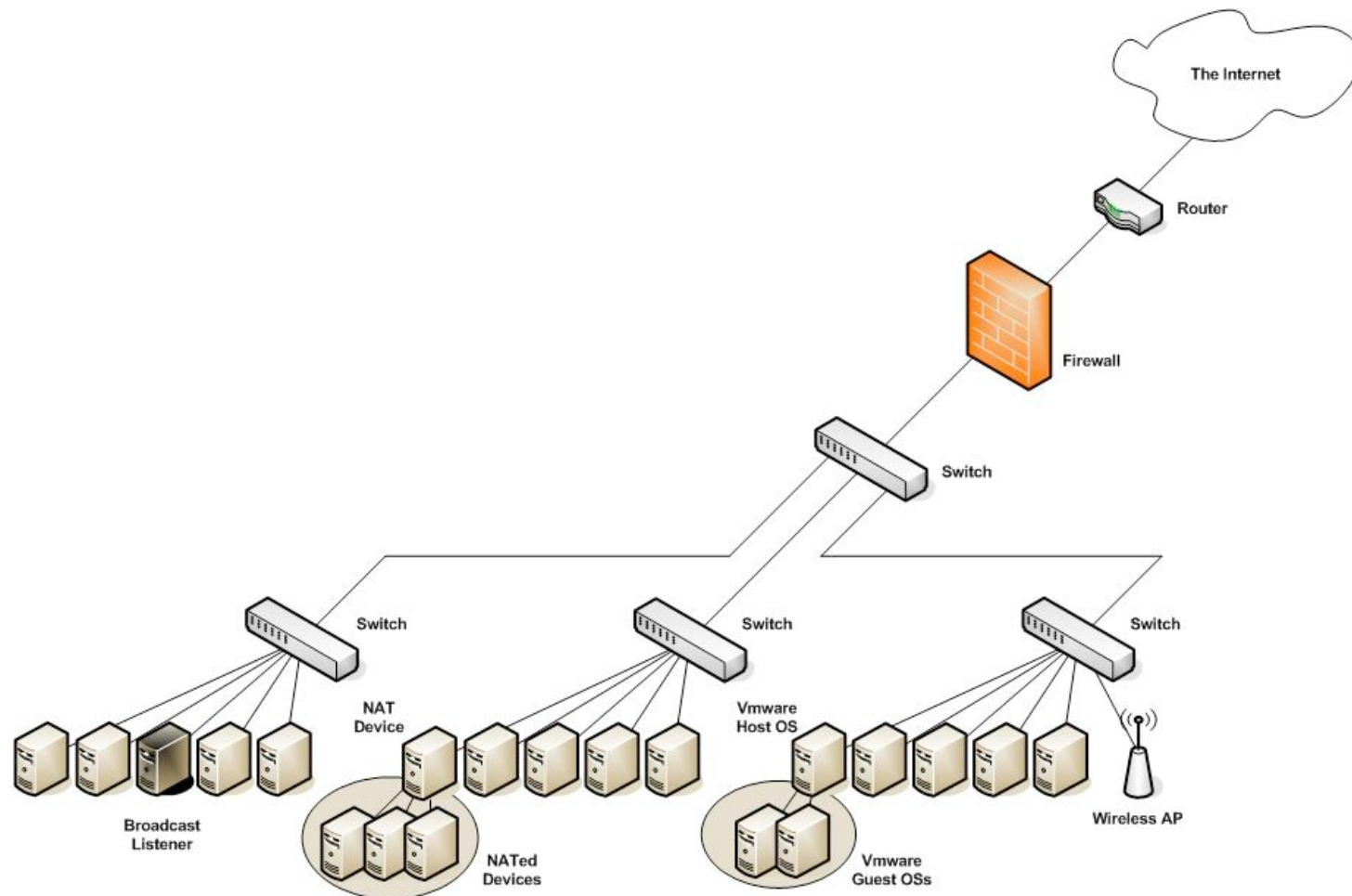
Weaknesses

- Not all elements on the enterprise network would use DHCP
- Exceptions needs to be manually inputted (i.e. printers)
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address and/or the IP address of an exception in order to receive full access to the enterprise network
- Not able to detect masquerading elements hiding behind an allowed elements (i.e. **NAT**)
 - Virtualization as a major issue (i.e. Freebee virtualization software such as Virtual PC, Vmware, etc.)

Broadcast Listeners

Broadcast Listeners

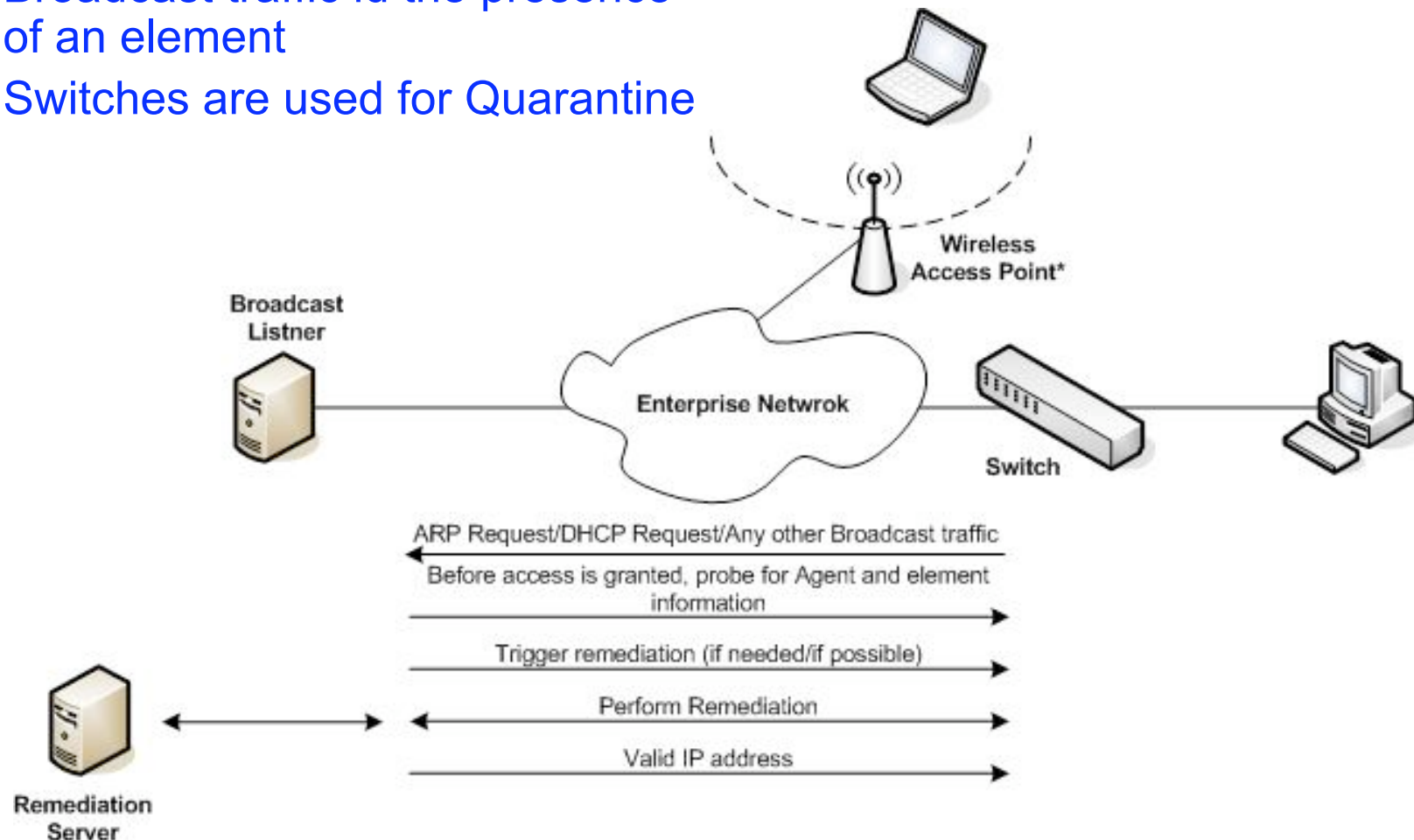
Architecture



Broadcast Listeners

Architecture: Managed Elements

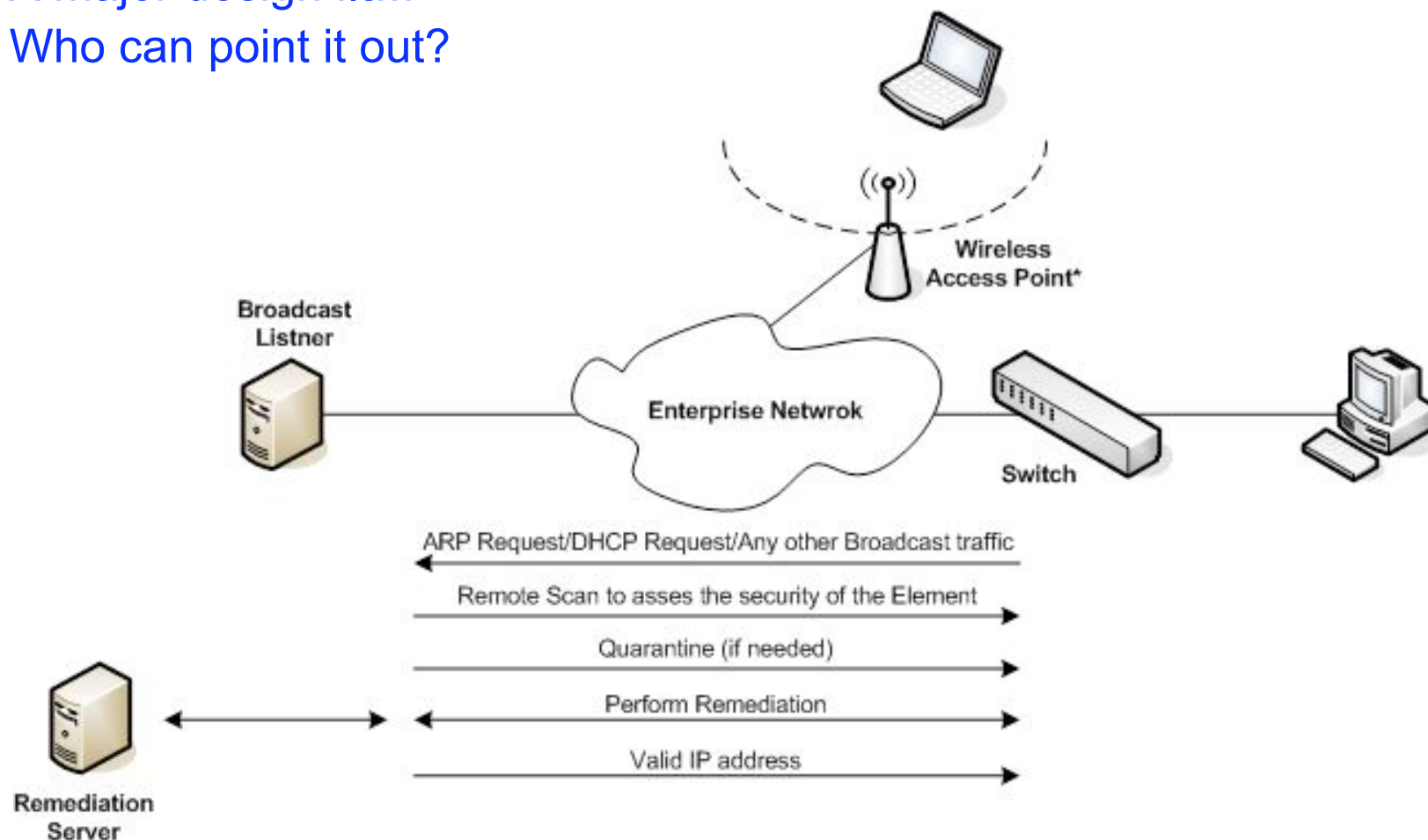
- Broadcast traffic id the presence of an element
- Switches are used for Quarantine



Broadcast Listeners

Architecture: Unmanaged Elements

- A major design flaw
- Who can point it out?



Broadcast Listeners

Unmanaged Elements

- Weaknesses
 - The element is already on the network
 - L3 enforcement and quarantine
 - The local subnet widely opened for an abuse

Broadcast Listeners

Weaknesses

- Software must be deployed on **each and every subnet**
 - A lot of moving parts
- **Prior knowledge** regarding the enterprise network must be obtained prior to deployment
 - What are the enterprise **subnets**?
 - Where are the **locations** to be deployed?
 - The approach of “the client tells us where to install the software” simply does not work

Broadcast Listeners

Weaknesses

- Must **integrate with switches** in order to perform **quarantine**
 - No knowledge **who these switches are**
 - In most cases the identification process of the switches might be a manual process
 - Switches may reside on **their own VLAN/Subnet**
 - Switches serving a certain subnet may reside on different subnets
 - In many cases switches can be **accessed only from a management network** (a sever deployment issue)
 - Read/Write access to switches is required
 - Understanding the VLAN structure might not be trivial.
 - VLAN hopping might be possible where multiple VLANs are defined on the same switch.
 - Appropriate VACLs must be introduced
- Rely on the switch to have the means to introduce quarantine and enforcement measures

Broadcast Listeners

Weaknesses

- No knowledge on actual network topology lead existence of other, **uncovered venues to access the network**
 - Other subnets which may not be monitored
 - Forgotten switches
- Not able to detect **masquerading elements** hiding behind an allowed elements (i.e. **NAT**)
 - Virtualization as a major issue (i.e. Freebee virtualization software such as Virtual PC, Vmware, etc.)
- Exceptions needs to be manually inputted
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address and/or the IP address of an exception in order to receive its access to the enterprise network
- Cannot be extended to include remote users

Broadcast Listeners

Weaknesses

- Unmanaged Elements
 - No Client-software for non-Windows operating systems
 - Non-Windows operating systems cannot be scanned for compliance (i.e. using a portal, client, Active-X, etc.)
 - External vulnerability scans takes time to complete
 - External vulnerability scans may fail
 - An increasing number of operating systems will be using a personal firewall. Remote scanning will **not reveal** information regarding the scanned elements
 - The number of exceptions would be high
- **Does not support** any form of **User Authentication**

Broadcast Listeners

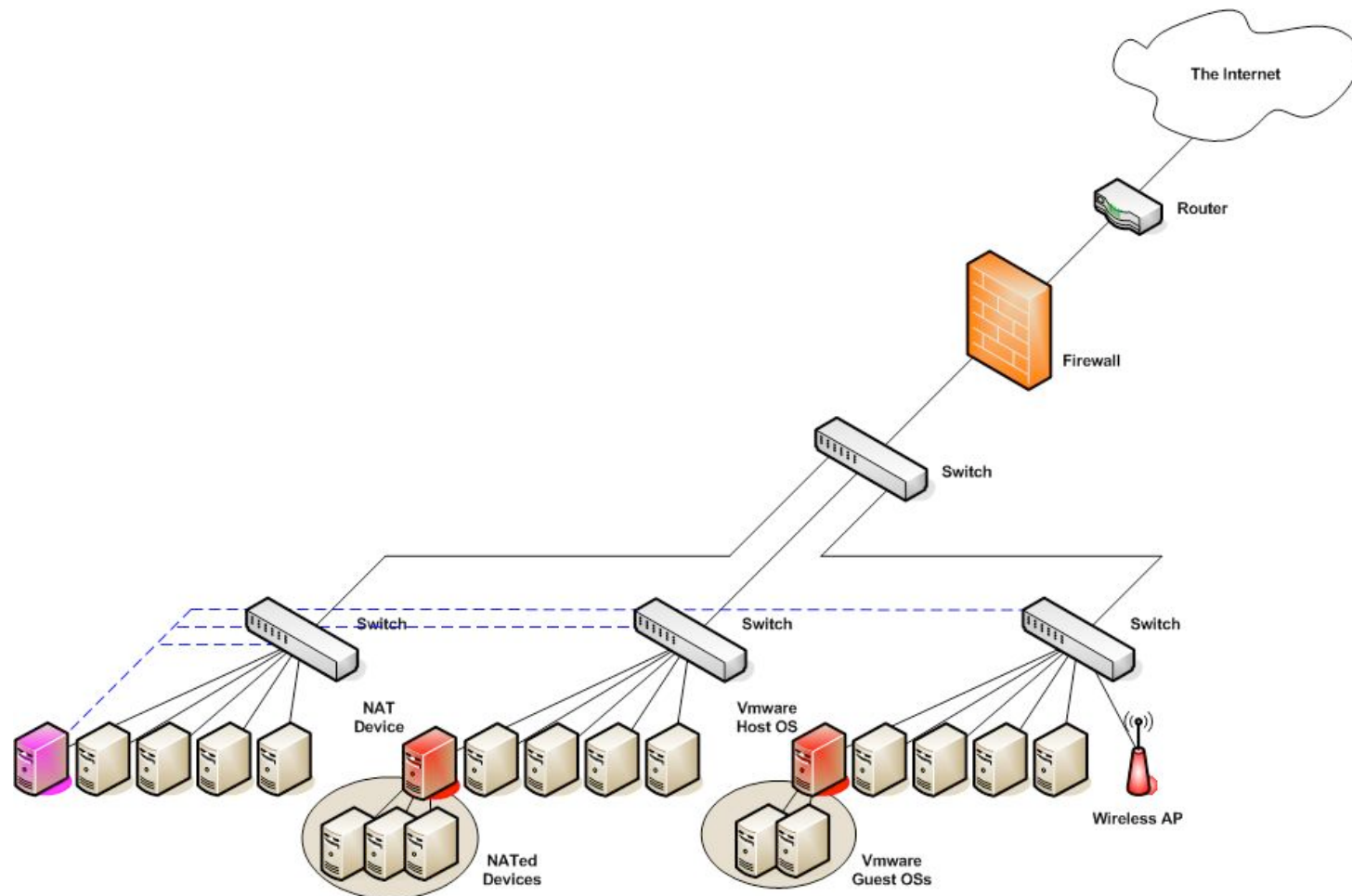
Weaknesses (Advanced)

- Some elements **may not generate broadcast traffic**
- **!** Configuring **static ARP entries** bypasses the detection of broadcast traffic
- **!** Abusing **manipulated ARP requests** bypasses the detection of broadcast traffic
 - Instead of aiming the request to the broadcast address, aim it directly to the MAC address you wish to communicate with
 - The destination element will be happy to communicate

Switch Integration

Switch Integration

Architecture



Switch Integration

Weaknesses

- Totally rely on the switch technology and capabilities to have the means to provide with a NAC solution
 - Element Detection
 - 802.1x
 - SNMP traps
 - Quarantine
 - Enforcement
 - Etc.
- Must **integrate with switches** operating on the enterprise network
 - No knowledge **who these switches are**
 - In most cases the identification process of the switches might be a manual process (no discovery capabilities)
 - Switches may reside on **their own VLAN/Subnet**
 - Switches serving a certain subnet may reside on different subnets
 - In many cases switches can be **accessed** only **from a management network** (a sever deployment issue)
 - Read/Write SNMP access to the switches is required

Switch Integration

Weaknesses

- Quarantine through the switch
 - Switches that do not support VLANs
 - Interoperability issues when the network is composed from multiple vendor networking gear
 - Understanding the VLAN structure might not be trivial.
 - VLAN hopping might be possible where multiple VLANs are defined on the same switch.
 - Appropriate VACLs must be introduced
- No form of user authentication
- Policy is defined per switch port and not per element
 - There is no ability to define a 'dynamic' policy according to the element, which connects to the network
- Multiple elements may not be able to be controlled if connected to the same switch port

Switch Integration

Weaknesses

- Not able to detect masquerading elements hiding behind allowed elements (i.e. **NAT**)
 - Virtualization as a major issue (i.e. Freebee virtualization software such as Virtual PC, Vmware, etc.)
- Any reference to an element is done using its MAC address
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address of an exception in order to receive its access to the enterprise network
- Cannot be extended to include remote users

802.1x

802.1x

- A username password based protocol
- For compliance checks must use an agent software
- Difficult manageability
 - All elements on the network must be configured to use 802.1x
 - **Legacy** networking gear must be upgraded to support 802.1x (or replaced)
- Not all of the networking elements can support 802.1x
- Not all of the elements residing on the network are 802.1x capable (i.e. legacy equipment, AS-400, printers, etc.)
- The **cost** for implementing a solution which is based on 802.1x is currently **high** (time, resources, infrastructure upgrade, etc.)

802.1x

- Exceptions
 - Hosts that do not support 802.1x can be granted access to the network using **manually configured exceptions** by MAC address
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address of an exception element in order to receive the **same access** that element has to the enterprise network
- Not able to detect masquerading elements hiding behind an allowed elements (i.e. **NAT**)
 - Virtualization as a major issue (i.e. Freebee virtualization software such as Virtual PC, Vmware, etc.)
- No knowledge on actual network topology may lead existence of other, uncovered venues to access the network
 - The network might be composed from other networking equipment which does not support 802.1x
 - Used as an access venue to the network

Switch Manufactures

Switch Manufactures

- Did where are my switches?
 - Before deployment a perfect understanding on how does the network looks like is a must
 - Networking gear from multiple manufactures
- Exception lists my dear Watson
- NAT
- Virtualization
- Cost

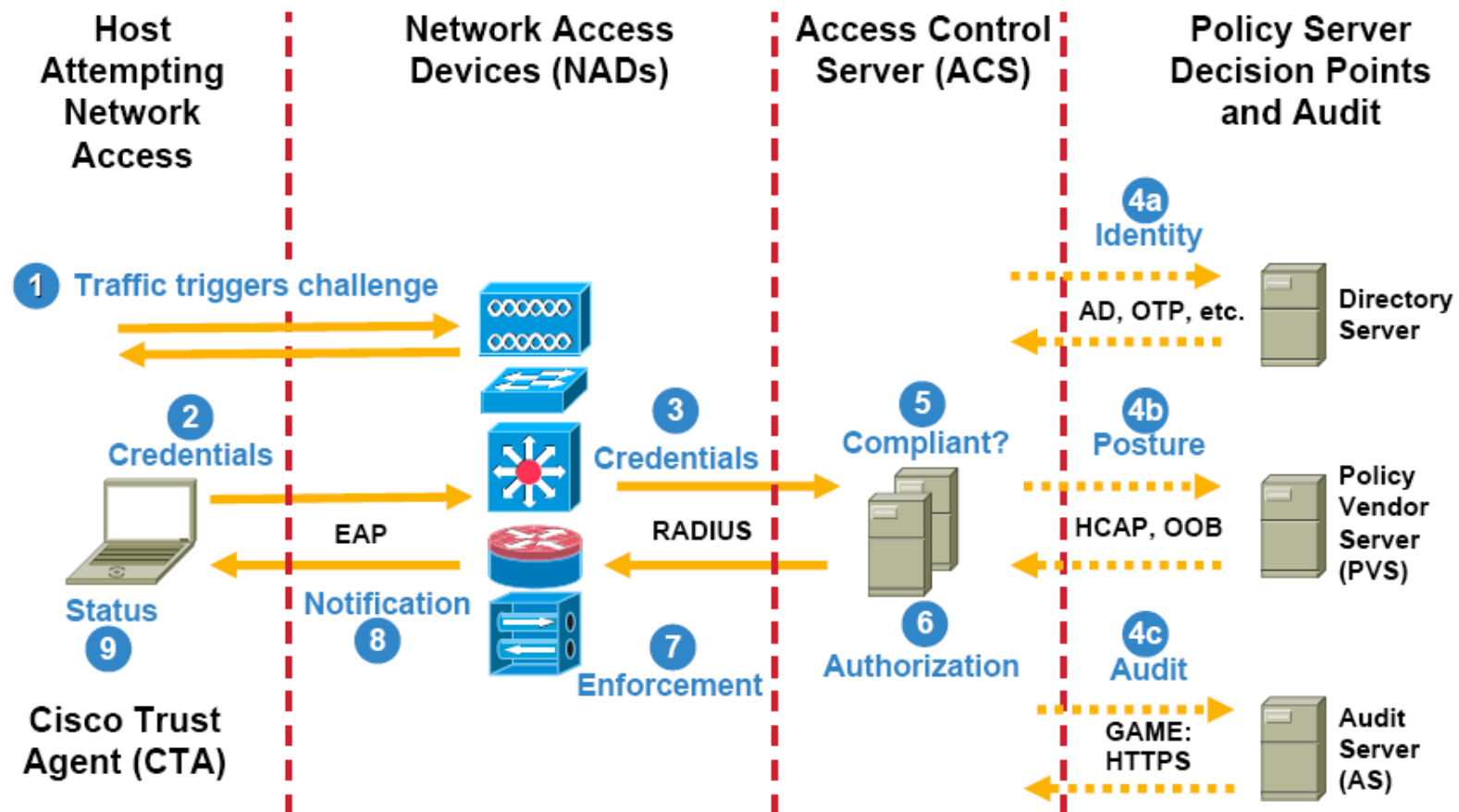
Cisco NAC Framework

Architecture

- Components
 - **C**isco **T**rust **A**gent (CTA)
 - Cisco **n**etwork **a**ccess **d**evice (NAD) with NAC enabled on one or more interfaces for network access enforcement
 - Cisco Secure **A**ccess **C**ontrol **S**erver (ACS) for endpoint compliance validation
- Enforcement strategies
 - NAC L3 IP
 - Deployed using Routers
 - Triggered by an **IP packet**
 - NAC L2 IP
 - Deployed using switches/routers
 - Apply per interface
 - Triggered by either a **DHCP packet** or an **ARP request**
 - NAC L2 802.1x
 - Triggered by any **data-link packet**

Cisco NAC Framework

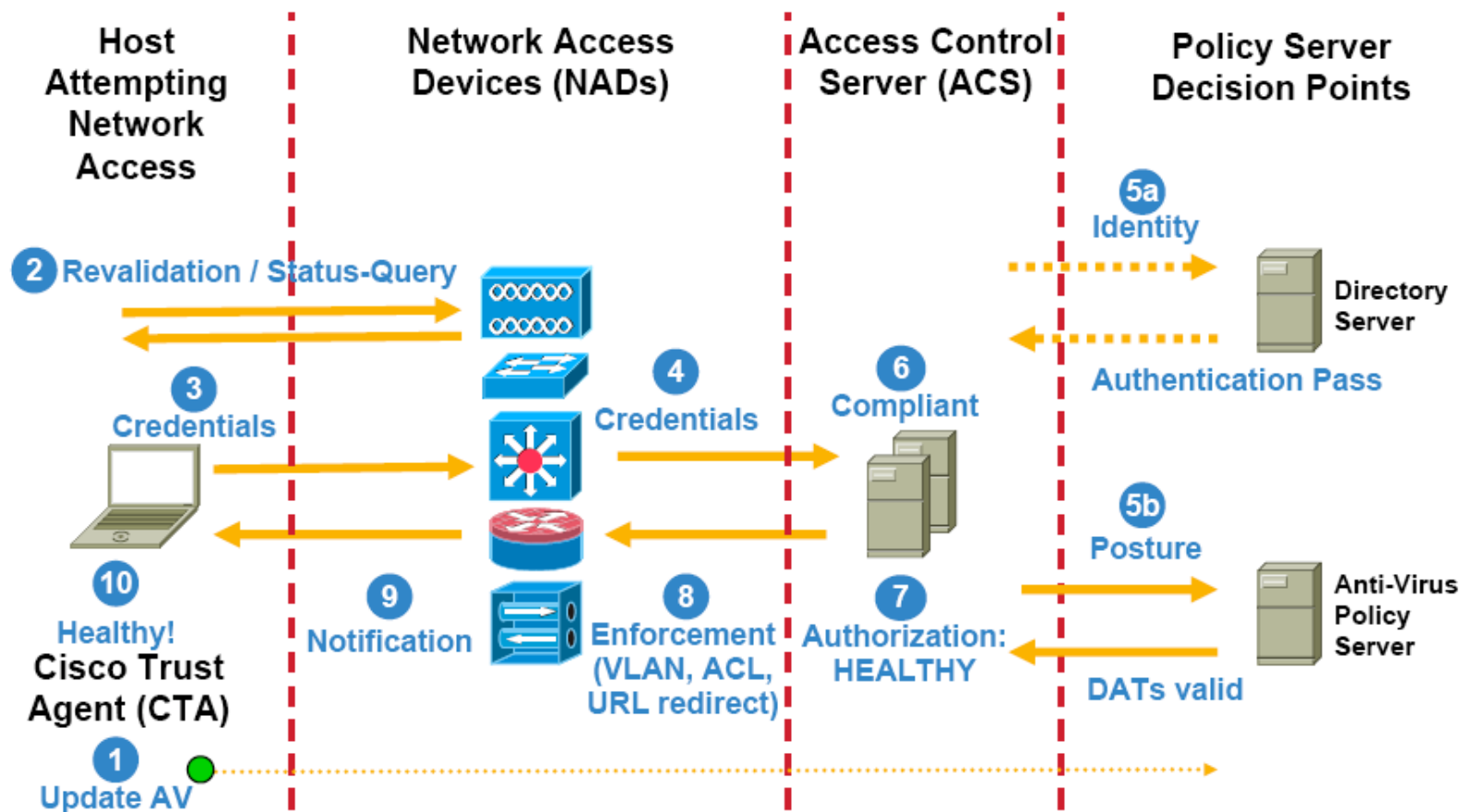
Information Exchange



Source: Cisco

Cisco NAC Framework

Information Exchange



Source: Cisco

Cisco NAC Framework

Strengths

- NAC L2 802.1x
 - Can prevent elements to connect to the network **even before assigned an IP address** (when implemented on switches)
 - **Embedded** with the underlying networking gear

Cisco NAC Framework

Weaknesses

- Works **only** with **Cisco equipment**
 - Only Cisco devices support the EAPoUDP protocol
- Difficult manageability
 - All elements on the network must be configured to use 802.1x
 - All the network elements on the network must be Cisco's
 - **Legacy** networking elements must be upgraded to support 802.1x
- Not all of the networking elements can support 802.1x
- Not all of the elements residing on the network are 802.1x capable (i.e. legacy equipment, AS-400, printers, etc.)
- The cost for implementing a solution which is based on 802.1x is currently high (time, resources, infrastructure upgrade, etc.)

Cisco NAC Framework

Weaknesses

- Not all of the enforcement strategies are bullet proof
 - NAC L3 IP
 - Deployed using Routers
 - Triggered by an **IP packet**
 - Local network is **vulnerable** to viruses, worms, and local compromises
 - NAC L2 IP
 - Apply per interface
 - Triggered by either a **DHCP packet** or an **ARP request**
 - Information might be **tunneled through**
 - Also applies when a hub is connected to the interface

Cisco NAC Framework Weaknesses

Unmanaged Elements

- Static Exceptions
 - “Hosts that cannot run the CTA (Cisco Trust Agent) can be granted access to the network using **manually configured exceptions** by MAC or IP address on the router or ACS. Exceptions by device types such as Cisco IP phones can also be permitted using CDP on the router. “ – Cisco NAC FAQ
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, and other properties)
 - It is possible to spoof the MAC address and/or the IP address of an exception in order to receive the **same access** that element has to the enterprise network

Cisco NAC Framework Weaknesses

Unmanaged Elements

- Dynamic Audit
 - “The newest component in the NAC solution is the audit server, which applies **vulnerability assessment** (VA) technologies to determine the level of compliance or risk of a host prior to network admission. “
 - The level of response from various elements is **questionable**
 - Many elements uses a personal firewall by default (even if the element is responsive, closing all “hatches” may still grant access to the network)

Cisco NAC Framework

Weaknesses

- Not able to detect masquerading elements hiding behind an allowed elements (i.e. NAT)
 - Virtualization as a major issue (i.e. Freebee virtualization software such as Virtual PC, Vmware, etc.)
- No knowledge on actual network topology may lead existence of other, uncovered venues to access the network
 - The network might be composed from different networking equipment from different companies other than Cisco

Cisco NAC Framework Weaknesses

Example: Default Quarantine ACL

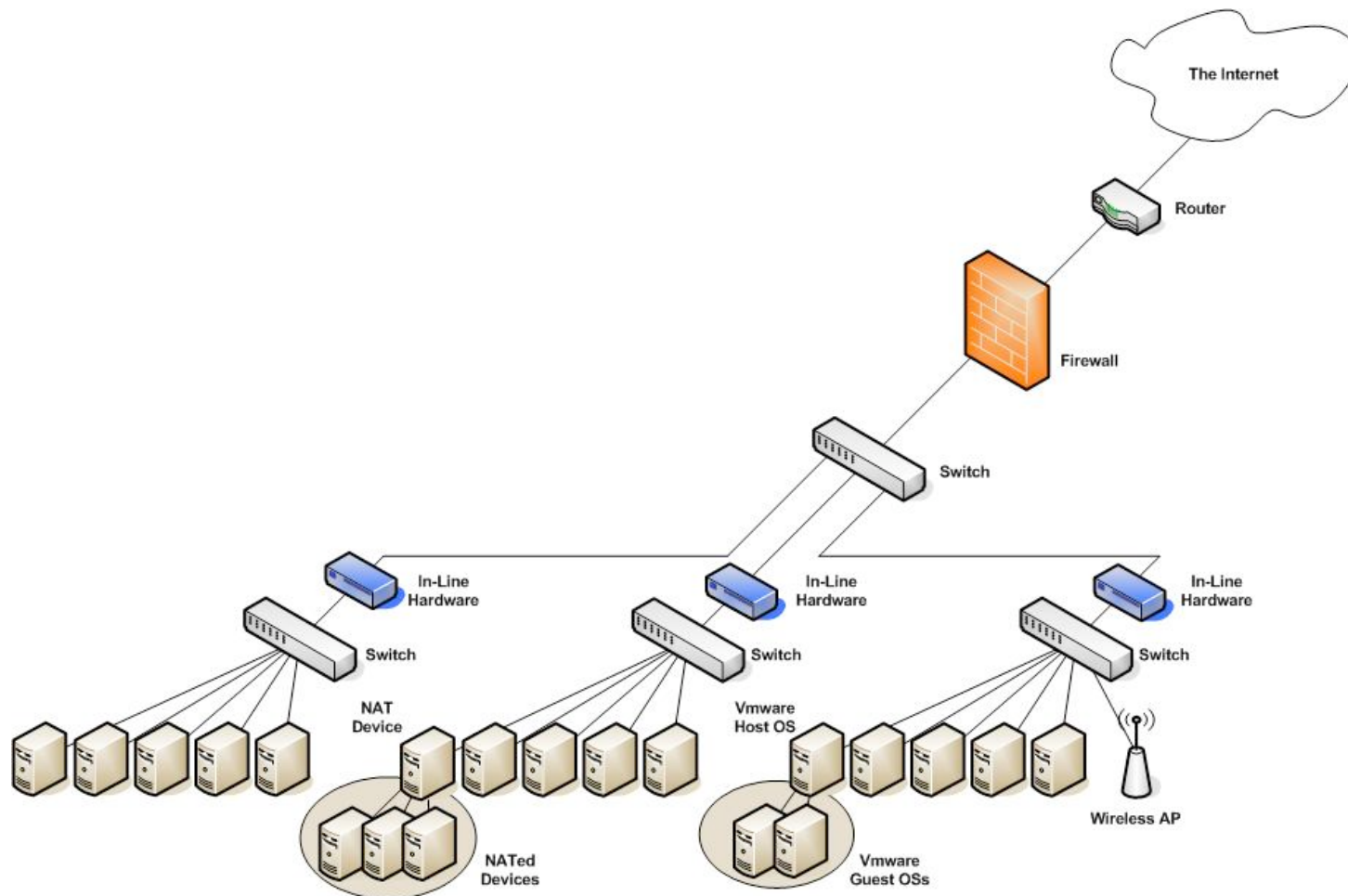
Name	NAF	ACL Definition
healthy_acl	(All-AAA-Client)	permit ip any any
quarantine_acl	(All-AAA-Client)	remark Allow DHCP permit udp any eq bootpc any eq bootps remark Allow EAPoUDP permit udp any any eq 21862 remark Allow DNS permit udp any any eq 53 remark Allow HTTP to UpdateServer permit tcp any host 10.0.200.30 eq www remark allow client access to qualys permit ip any host 10.0.200.106

Source: Network Admission Control (NAC) Framework Configuration Guide, Cisco

In-Line Devices

In-Line Devices

Architecture



In-Line Devices

Weaknesses

- No knowledge on actual network topology may lead existence of other, uncovered venues to access the network
 - Where to install the in-line devices?
- Deployment must involve a **network re-architecture** (also a political issue)
- Non-networking gear in a networking environment
- Deployment must be **as close as possible to the access layer** to be efficient and productive
- A possible **point of failure**
- Deployment is time consuming (the networking people in IT would fiercely resist it)
- The **infection/compromise** of other elements on the **local subnet** and/or switch is possible
- Some elements may only generate Layer 2 traffic
- Bandwidth limitation (most supports only 1GB/sec)
- Cost

In-Line Devices

Weaknesses

- **Element detection** is performed **at Layer 3** only
 - Elements can infect and/or penetrate other elements on their local subnet, and cannot be stopped
 - If elements are detected due to their IP traffic (rather than according to their Layer 2 traffic) there would be many different venues to bypass the in-line device
 - If elements are detected due to their broadcast traffic, it is still possible to bypass the in-line device's element detection capabilities (see: Broadcast Listeners)
 - Bypassing enforcement by attacking a system on the local subnet using it as an 'access proxy' to other parts of the enterprise network
 - With many IT networks servers will share the same subnet with desktops
- Encryption

In-Line Devices

Weaknesses

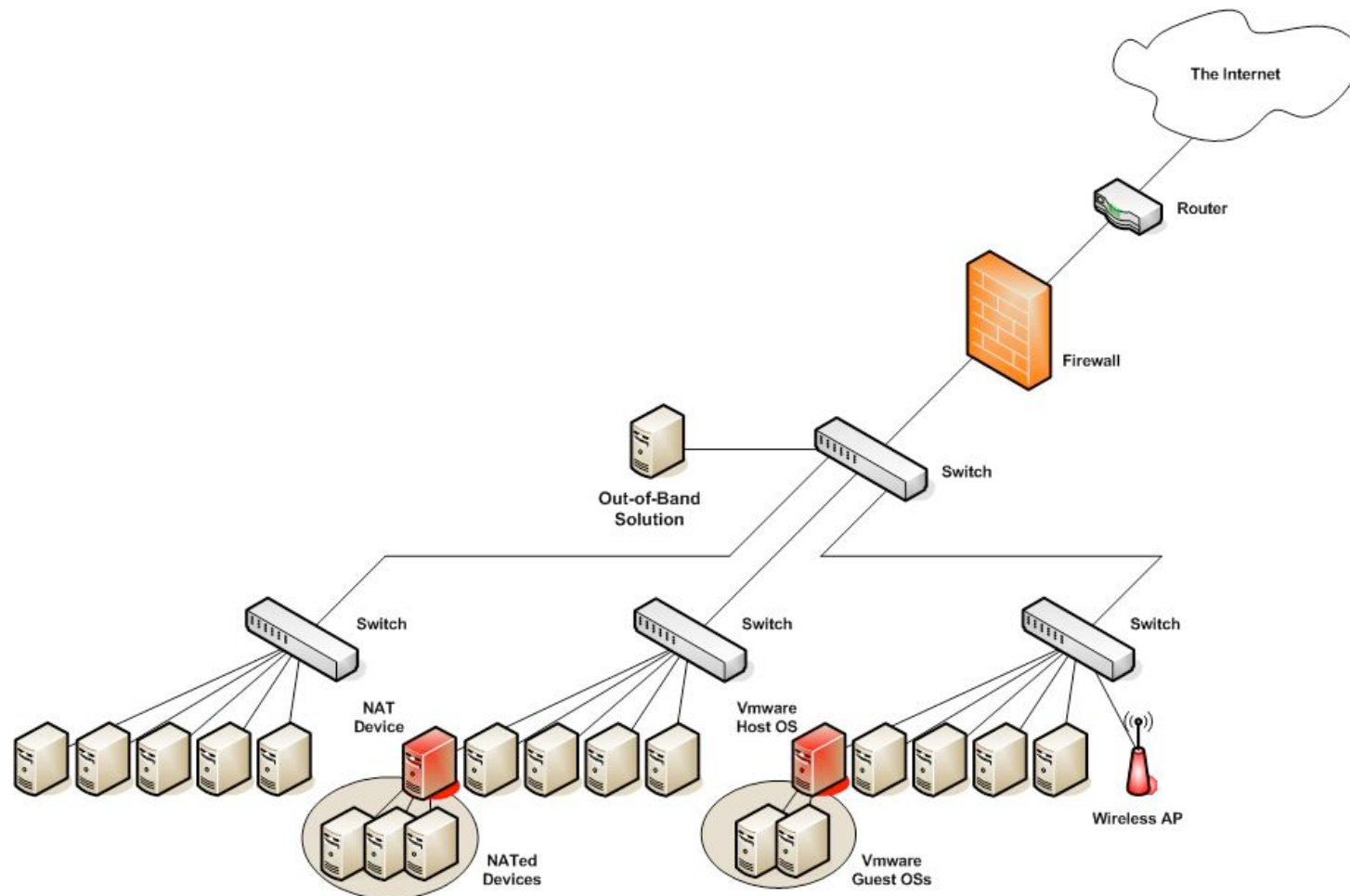
- Not able to detect smart masquerading
 - Using the same underlying operating system as the NAT service provider will completely hide the NATed element (i.e. using random ID numbers, etc.)
- Exceptions needs to be manually inputted (i.e. printers)
 - There is **no knowledge** about the **exception element** (i.e. OS, exact location, functionality, and other properties)*
 - It is possible to spoof the MAC address and/or the IP address of an exception in order to receive its access to the enterprise network

* If the operating system of the element is being tracked, mimicking the OS responses would yield the same access rights to the network

Out-of-Band Devices

Out-of-Band Devices

Architecture



Out-of-Band Devices

Strengths

- Fast to implement
- Less moving parts
- Real-time
- Detection at L2 (if deployed close enough to the access layer)

Out-of-Band Devices

Weaknesses

- Incomplete discovery
 - Inactive elements will not be detected
- As long as the traffic generated is not broadcast traffic and does not pass through the monitoring point of the out-of-band solution, the element would not be detected
- May suffer from the different issues as Broadcast Listeners
- For more issues please see: **Risks of Passive Network Discovery Systems (PNDS)**, Ofir Arkin, 2005. Available from: <http://www.insightix.com/resources/whitepapers.html>

The End Result

The End-Result

- A confused market place
- Solutions are being bought without proper verification and checking
- Most of the available NAC solutions on the market today can be bypassed
- We are starting to see a more serious attitude towards the pitfalls of various NAC solutions outlined in the 'bypassing NAC' presentation

Questions?

Resources

- Microsoft NAP
<http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx>
- Cisco NAC
http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- TCG
<https://www.trustedcomputinggroup.org/home>
- Insightix
<http://www.insightix.com>
- The Sys-Security Group
<http://www.sys-security.com>

Thank You