August 2007

kNAC!

10 (or more) ways to bypass a NAC solution





Ofir Arkin, CTO

insightix
Keep your network in sight

www.insightix.com

In Memory of Oshri Oz



September 13, 1972 - May 27, 2007

© Ofir Arkin, 2006 - 2007

Agenda

- What is NAC?
- NAC Basics
- 10 (or more) ways to bypass NAC

© Ofir Arkin, 2006 - 2007

Ofir Arkin

- CTO & Co-Founder, Insightix
  http://www.insightix.com
- Founder, The Sys-Security Group
  http://www.sys-security.com
- Computer security researcher
  - Infrastructure discovery
    - ICMP Usage in Scanning
    - Xprobe2
  - VoIP security
  - Information warfare
  - NAC

© Ofir Arkin, 2006 - 2007

What is NAC?

© Ofir Arkin, 2006 - 2007

What is NAC?

- What problem does it aim to solve?
- What functions does it need to support?
- What type of a solution is it?
  - A compliance solution?
  - A security solution?

© Ofir Arkin, 2006 - 2007

The Problem

© Ofir Arkin, 2006 - 2007

The Problem

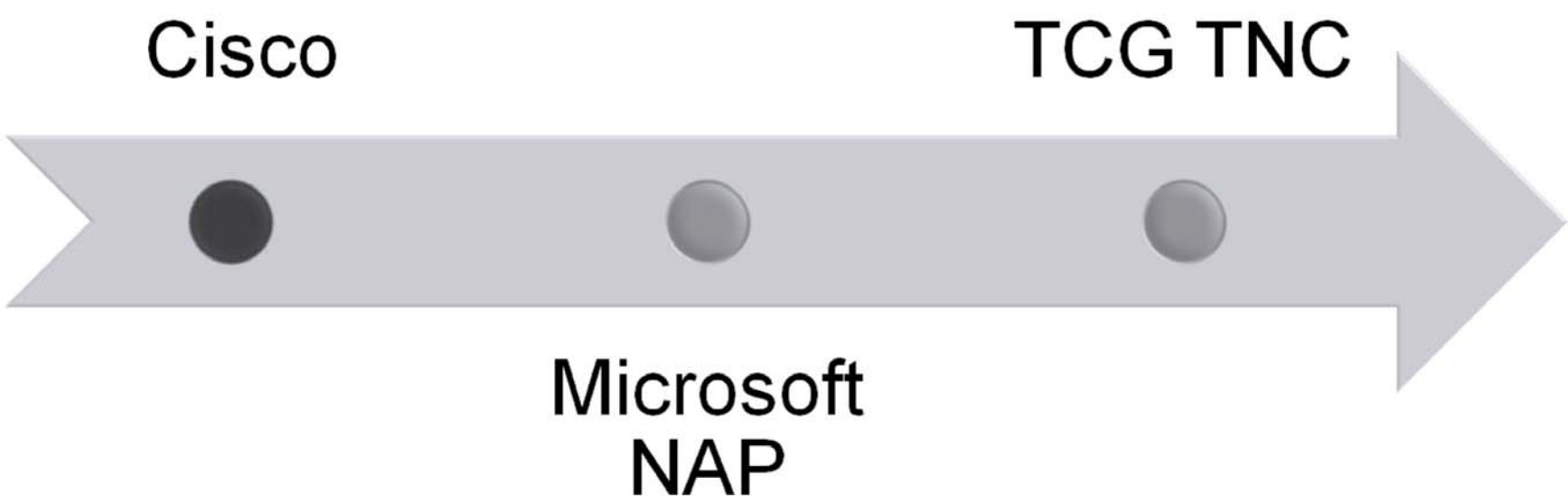
- An enterprise network is a complex and dynamic environment which hosts a variety of devices
  - Workstations, servers, printers, wireless access points, VoIP phones, switches, routers and more
- The stability, integrity and the regular operation of the enterprise LAN are in jeopardy by rogue, non-compliant and unmanaged elements (viruses, worms, Malware, information theft, etc.)

© Ofir Arkin, 2006 - 2007

NAC History

© Ofir Arkin, 2006 - 2007

NAC History



© Ofir Arkin, 2006 - 2007

What is NAC?

© Ofir Arkin, 2006 - 2007

What is NAC?

- Standardization and/or common criteria for NAC does not exist
- 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

© Ofir Arkin, 2006 - 2007

What is NAC?

- The basic task of NAC is to control network 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

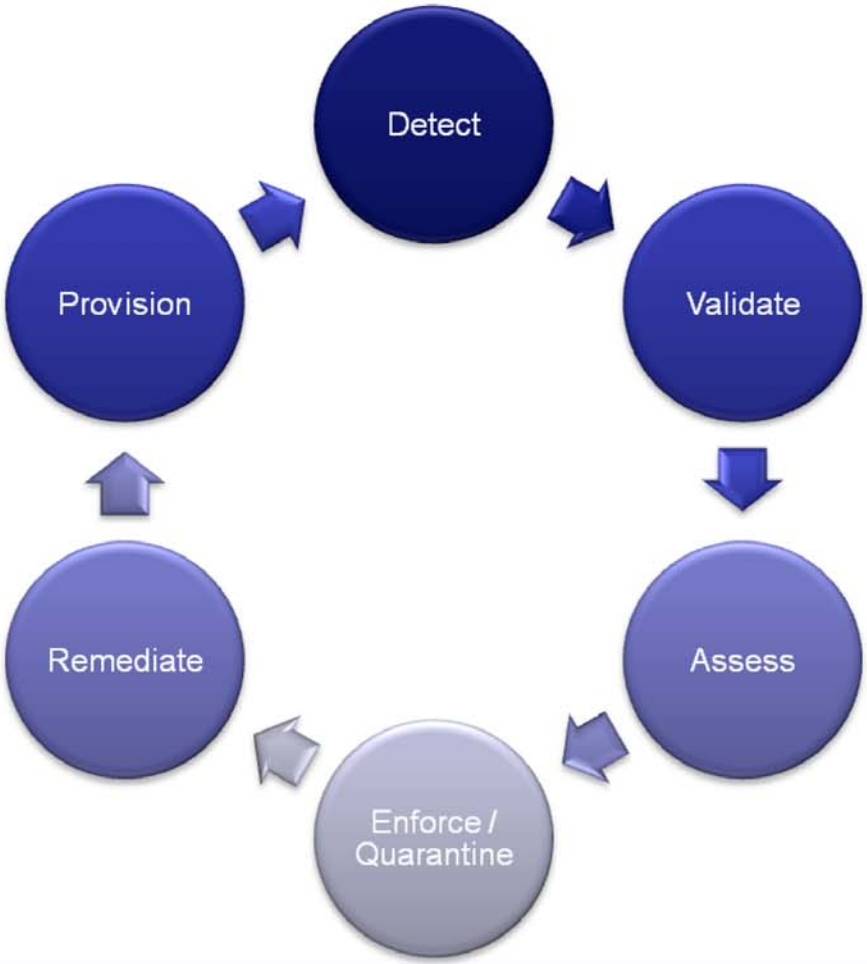
© Ofir Arkin, 2006 - 2007

My Definition of NAC

- **N**etwork **A**ccess **C**ontrol (NAC) is a set of technologies and defined processes, which are tasked with controlling access to the Enterprise LAN allowing only authorized and compliant devices to access and operate on the network

© Ofir Arkin, 2006 - 2007

NAC Basics



© Ofir Arkin, 2006 - 2007

Attack Vectors

© Ofir Arkin, 2006 - 2007

Attack Vectors

- Architecture
  - The inner working of the different solution pieces
- Technology
  - The technology used to support the various NAC features
    - Element detection
    - Device authorization
    - User authentication
    - Assessment
    - Quarantine / Enforcement
    - Etc.
- Components
  - The various components a solution is combined from

© Ofir Arkin, 2006 - 2007

10 (or more) ways to bypass NAC

© Ofir Arkin, 2006 - 2007

Ways to Bypass NAC

- Definition
- Element detection
  - Completeness
  - Real-time
  - L2 vs. L3
- Validation
  - Device authorization
  - User authentication
- Quarantine
  - Shared Vs. Private
  - L2 vs. L3
  - How to bypass

© Ofir Arkin, 2006 - 2007

Ways to Bypass NAC

- Enforcement
  - Using exceptions as a bypass means
  - L2 vs. L3
- Assessment
  - Qualification of elements
  - Client vs. client less
  - All-in-one client approach
  - The information checked as part of the assessment stage
  - Falsifying returning information

© Ofir Arkin, 2006 - 2007

The Definition

© Ofir Arkin, 2006 - 2007

Definition

- The problem definition
- How one defines its NAC solution
- The goal of the NAC solution
  - Posture validation only
  - Access control against all devices
- How does the NAC solution defined?
  - Security
  - Compliance

© Ofir Arkin, 2006 - 2007

Definition

- "Trusted Network Connect (TNC)…is an open, nonproprietary standard that enables the application and enforcement of security requirements for endpoints connecting to the corporate network…enforce corporate configuration requirements and to prevent and detect malware outbreaks…"
- "TNC includes collecting endpoint configuration data; comparing this data against policies set by the network owner; and providing an appropriate level of network access based on the detected level of policy compliance"

© Ofir Arkin, 2006 - 2007

Element Detection

© Ofir Arkin, 2006 - 2007

Element Detection

- THE core feature of any NAC solution
- One cannot afford having an element operating on its network without knowing about it
- If a NAC solution cannot perform complete element detection in real-time then it does not provide a valuable line of defense
- No Knowledge == No Control == No Defense
- No Element Detection == No NAC

© Ofir Arkin, 2006 - 2007

Multitude of Element Detection Methods

- Listening to traffic
  - DHCP
  - Broadcast listeners
  - Out-of-band solutions
  - In-line devices
- Through an integration with a switch
  - 802.1x
  - SNMP traps
- Software
  - Client-based software

© Ofir Arkin, 2006 - 2007

Multitude of Element Detection Methods

L2	L3	Switch	Software
Broadcast listeners	DHCP	802.1x	Agents
In line devices	In line devices	SNMP traps	
Out of band solutions	Out of band solutions		

© Ofir Arkin, 2006 - 2007

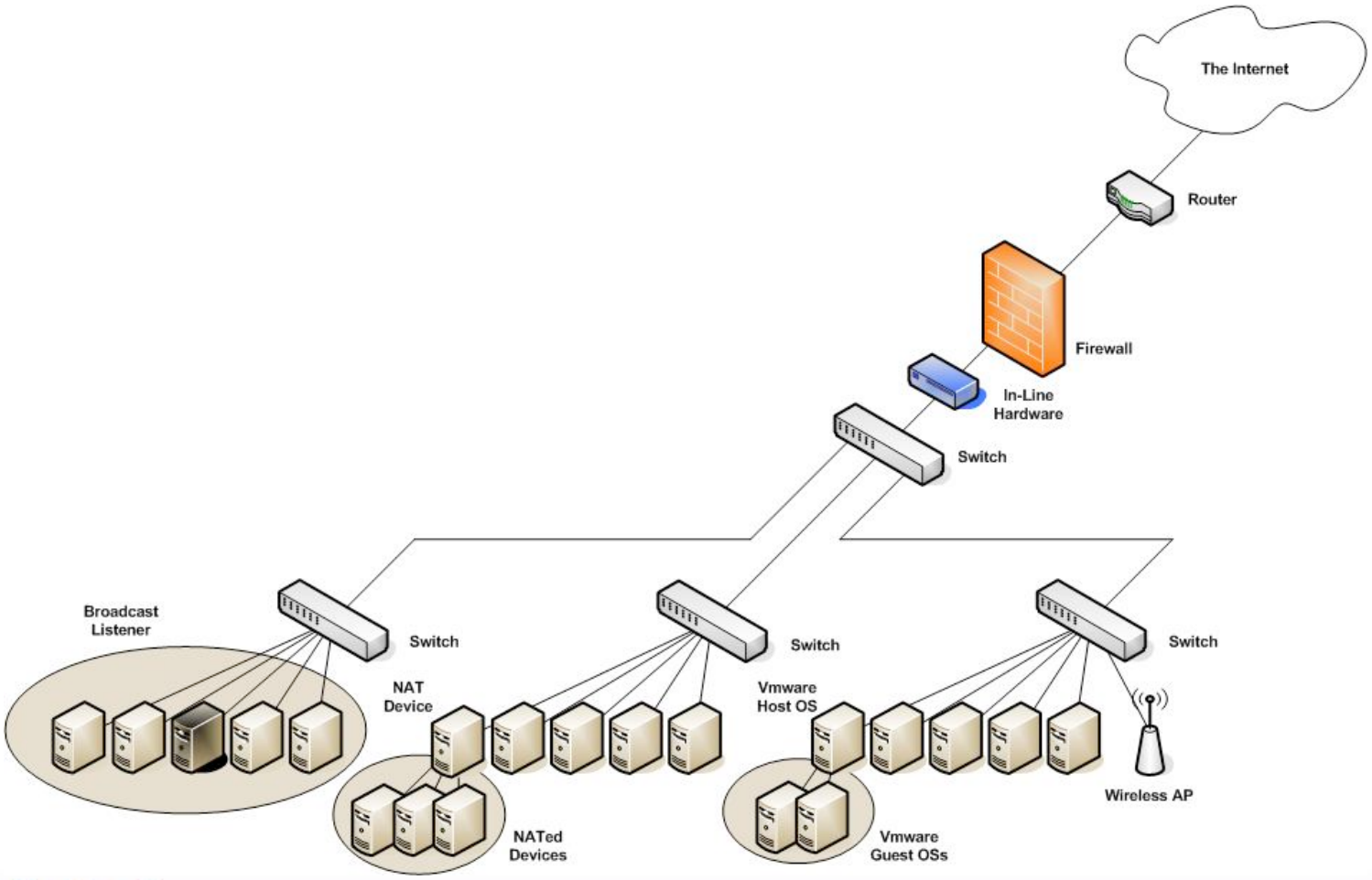
Passive Element Detection

- What you see is only what you get
  - A passive network discovery and monitoring solution cannot draw conclusions about an element and/or its properties if the related network traffic does not go through the monitoring point
- No control over the pace of the discovery
  - One cannot force an element to send traffic (passively)

- More information:
  - “Risks of passive network discovery systems”, Ofir Arkin, 2005. Available from: http://sys-security.com/blog/published-materials/papers/

© Ofir Arkin, 2006 - 2007

Passive Element Detection, L2 & L3 Example



© Ofir Arkin, 2006 - 2007

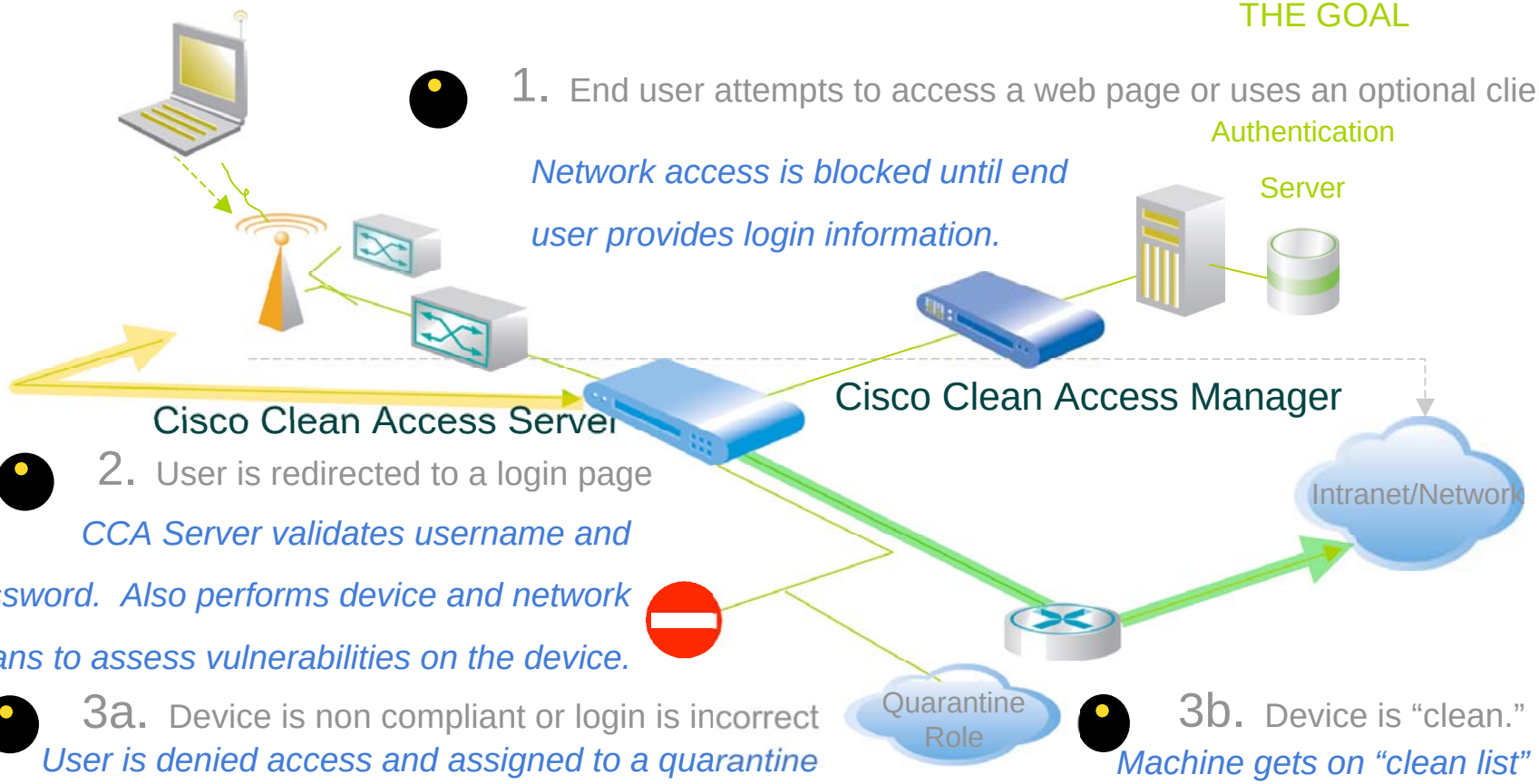
Passive Element Detection

- Layer-3
  - Not real-time
    - You cannot expect an element to send traffic through the monitoring point as soon as it is introduced to the network (or to send the type of traffic the solution needs at all…)
  - Not complete
    - One cannot force an element to send traffic (passively)
  - An element can reside on the local subnet and not be detected
- Layer-2
  - An element may reside on the local subnet and not be detected

© Ofir Arkin, 2006 - 2007

Issues with Element Detection L3 Example

Source: Cisco Clean Access presentation

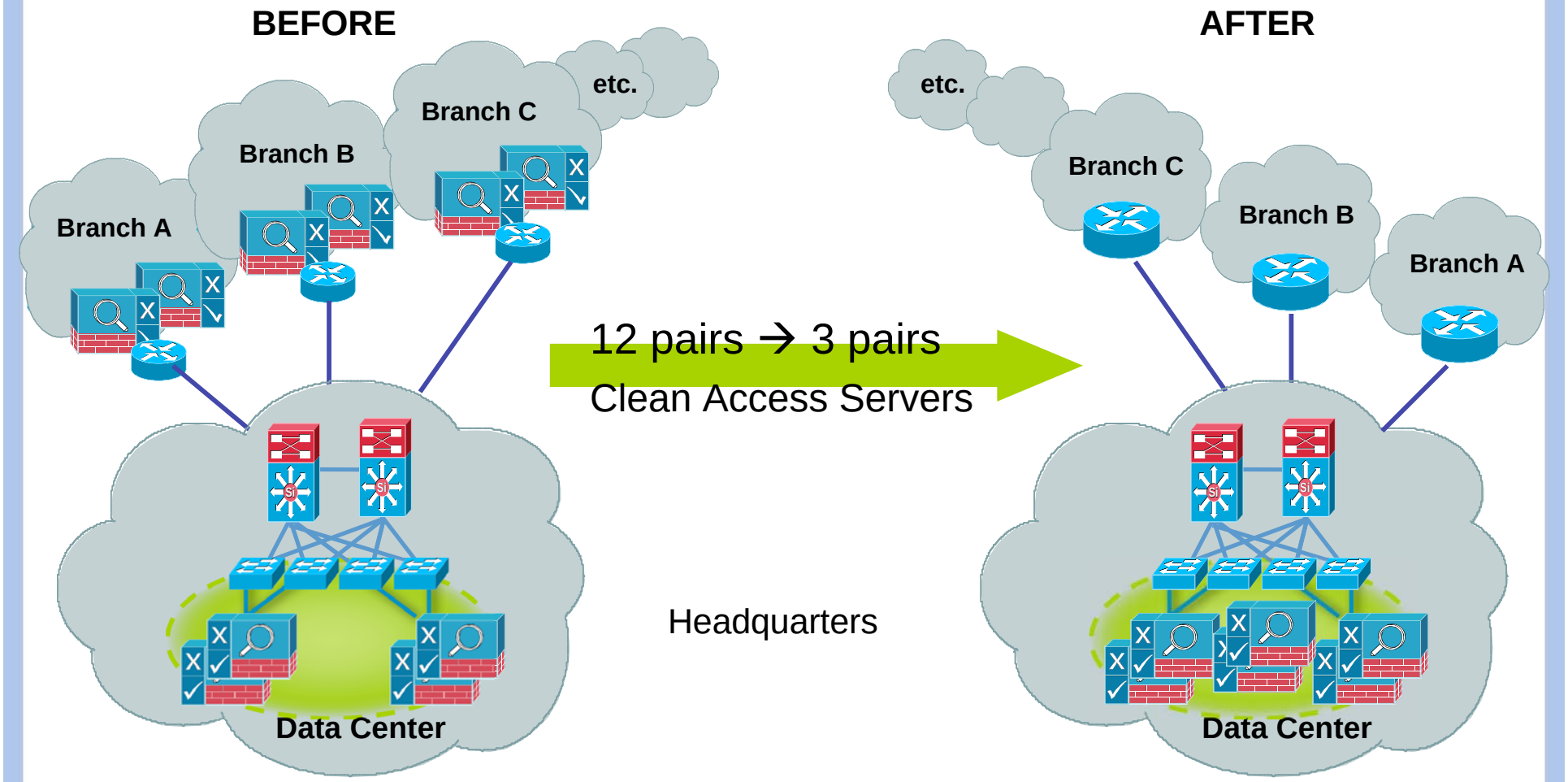


© Ofir Arkin, 2006 - 2007

Issues with Element Detection L3 Example

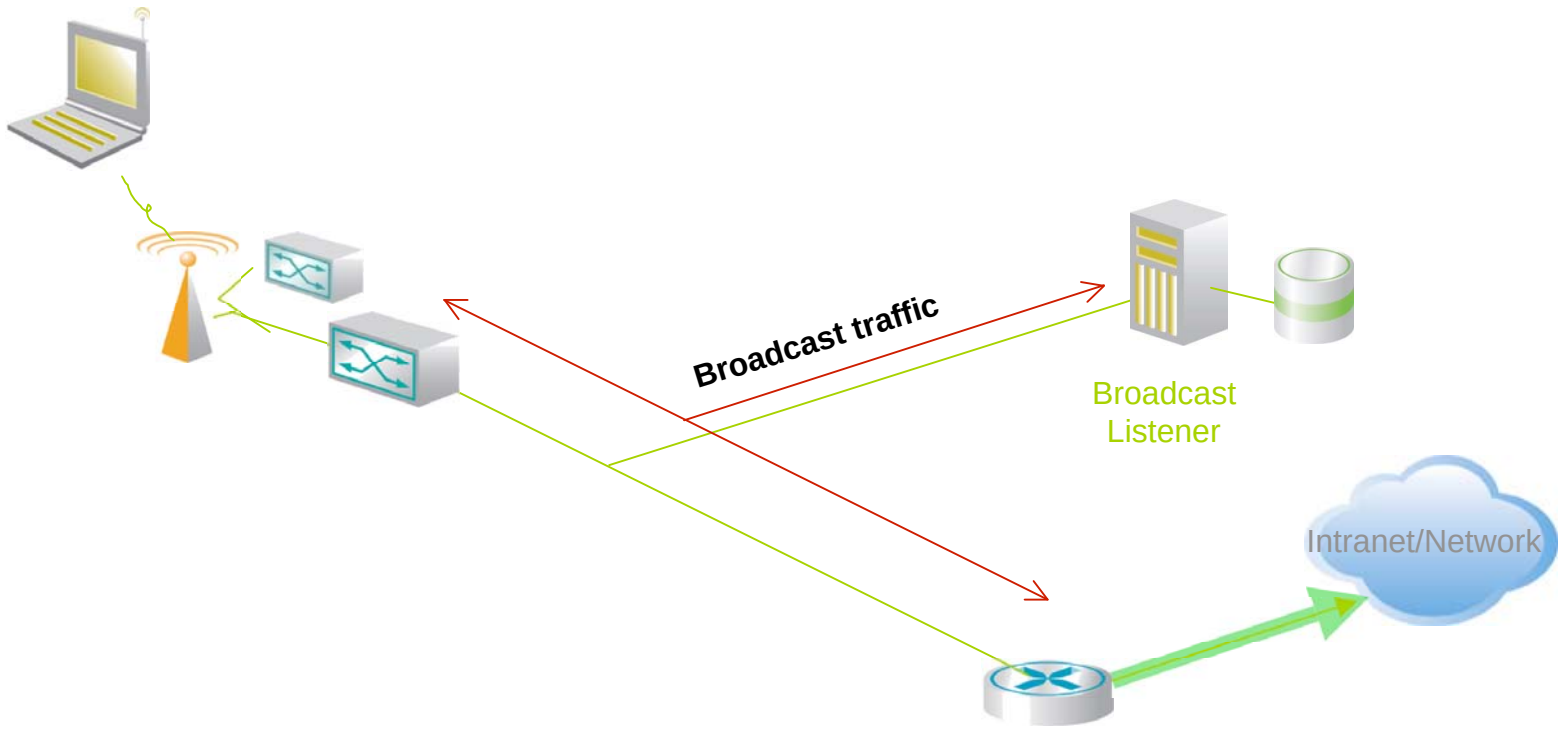
Source: Cisco Clean Access presentation

Scenario: 1 Headquarters with 3,000 users & 10 Branches with 1,000 users total



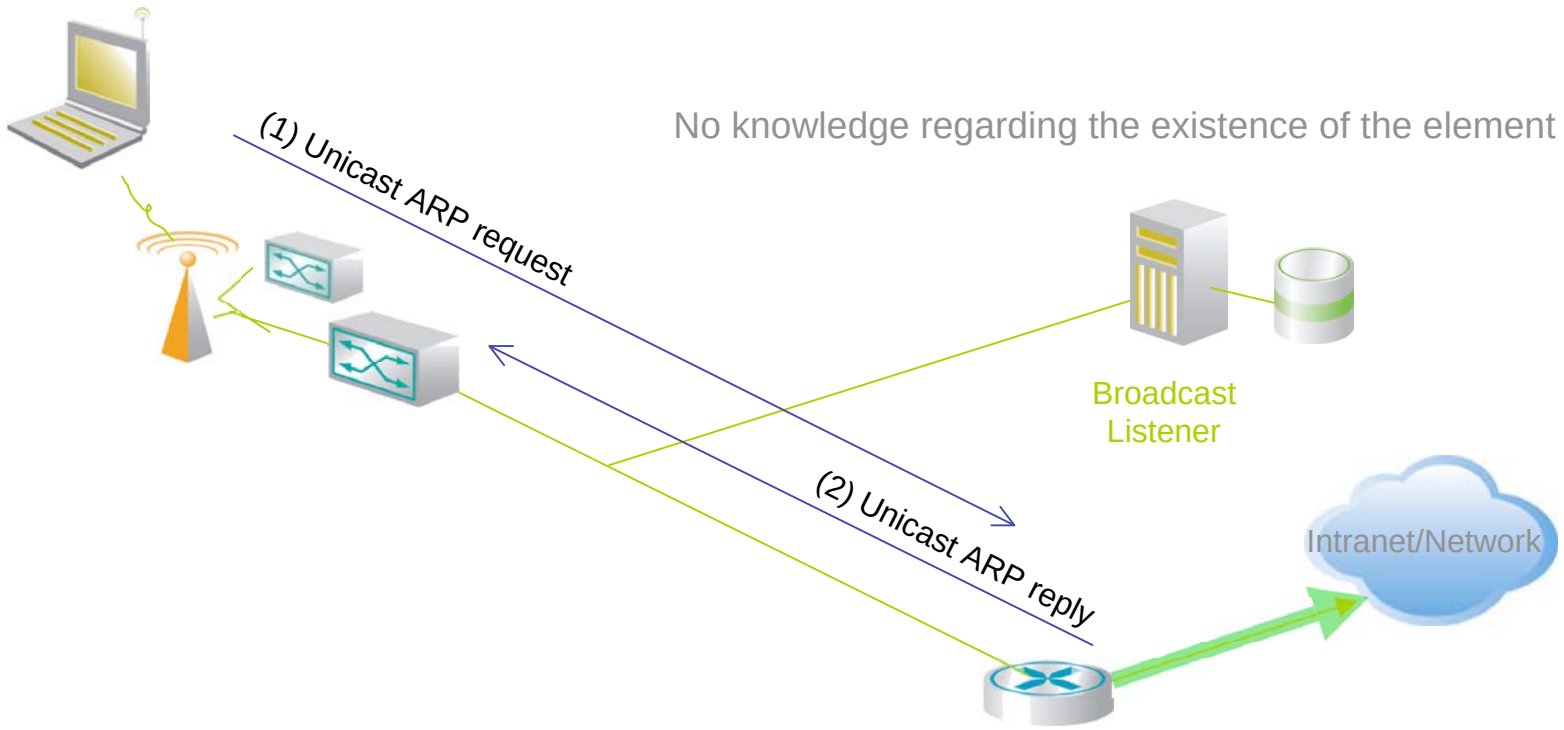
© Ofir Arkin, 2006 - 2007

Issues with Element Detection L2 Example



© Ofir Arkin, 2006 - 2007

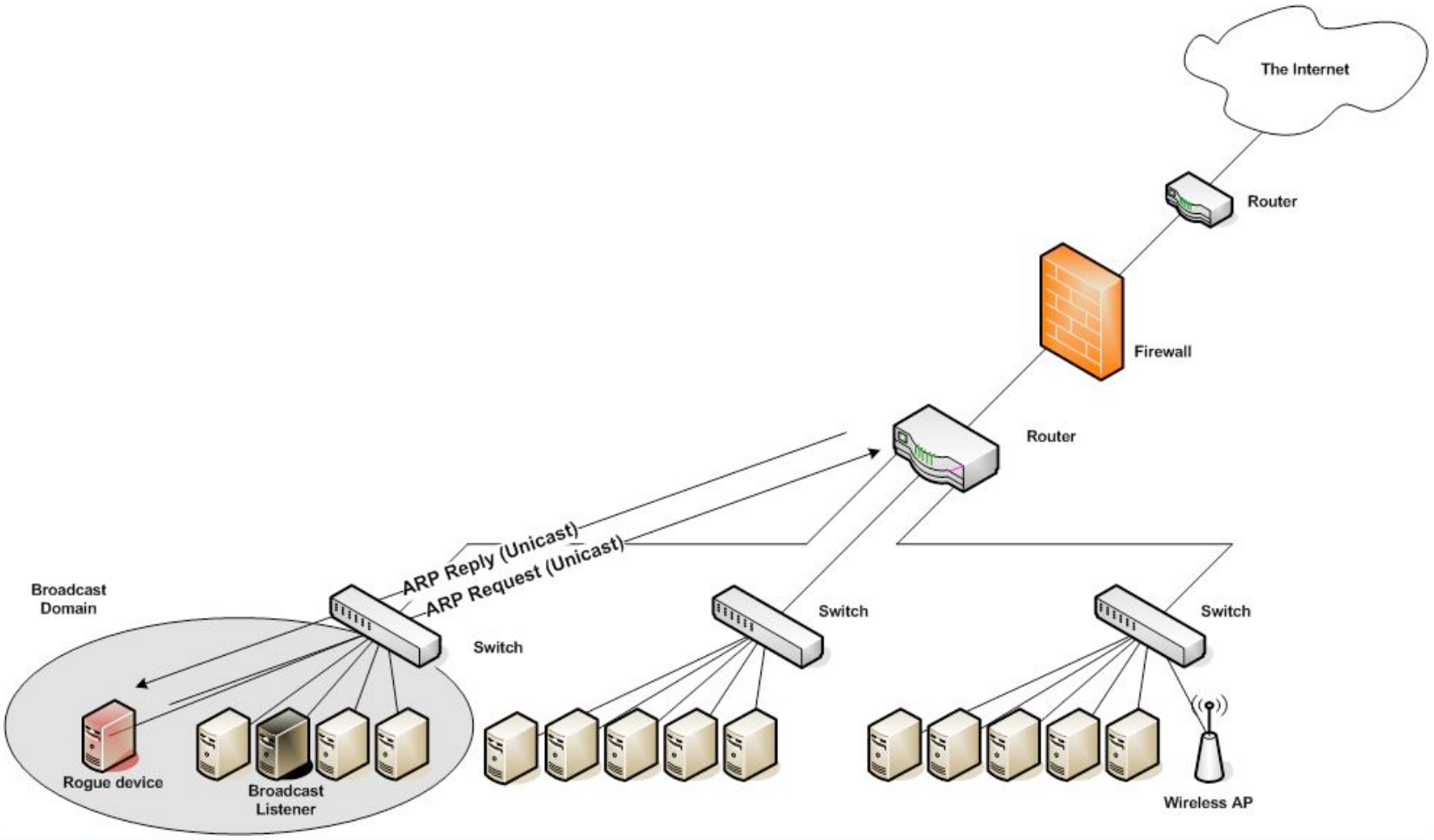
Issues with Element Detection L2 Example



© Ofir Arkin, 2006 - 2007

Issues with Element Detection L2 Example

Product: (Can one guess?)



© Ofir Arkin, 2006 - 2007

Other Element Detection Issues

- Some element detection methods provides with poor discovery capabilities
  - DHCP: Elements which do not use DHCP will not be discovered
  - SNMP Traps: Elements connecting to switches which cannot send SNMP traps in regards to new Source MAC registrations will not be discovered
  - Client Software: Elements which cannot install the client-based software will not be discovered

© Ofir Arkin, 2006 - 2007

Other Element Detection Issues

- Most element detection methods will not discover
  - NAT enabled devices
  - NAT in progress
- Virtualization makes a huge problem
  - Vmware
  - Xen
  - Parallels
  - Etc.

© Ofir Arkin, 2006 - 2007

Validation

© Ofir Arkin, 2006 - 2007

Validation

- Validation is the process of authorizing devices to operate on the Enterprise LAN and proving the identity of their users (as users which belong to the organization and allowed to use its network)

© Ofir Arkin, 2006 - 2007

Validation

- The role of device authorization is to combat rogue devices and to make sure that only authorized devices operates on the Enterprise LAN
- It must be tightly integrated with element detection
- If a device is unauthorized, its access to the network must be immediately blocked when it is being attached to the network
- Most NAC solutions will not authorize devices (some would only authenticate users)
- And nearly all NAC solutions are not able to perform complete and real-time element detection

© Ofir Arkin, 2006 - 2007

Validation

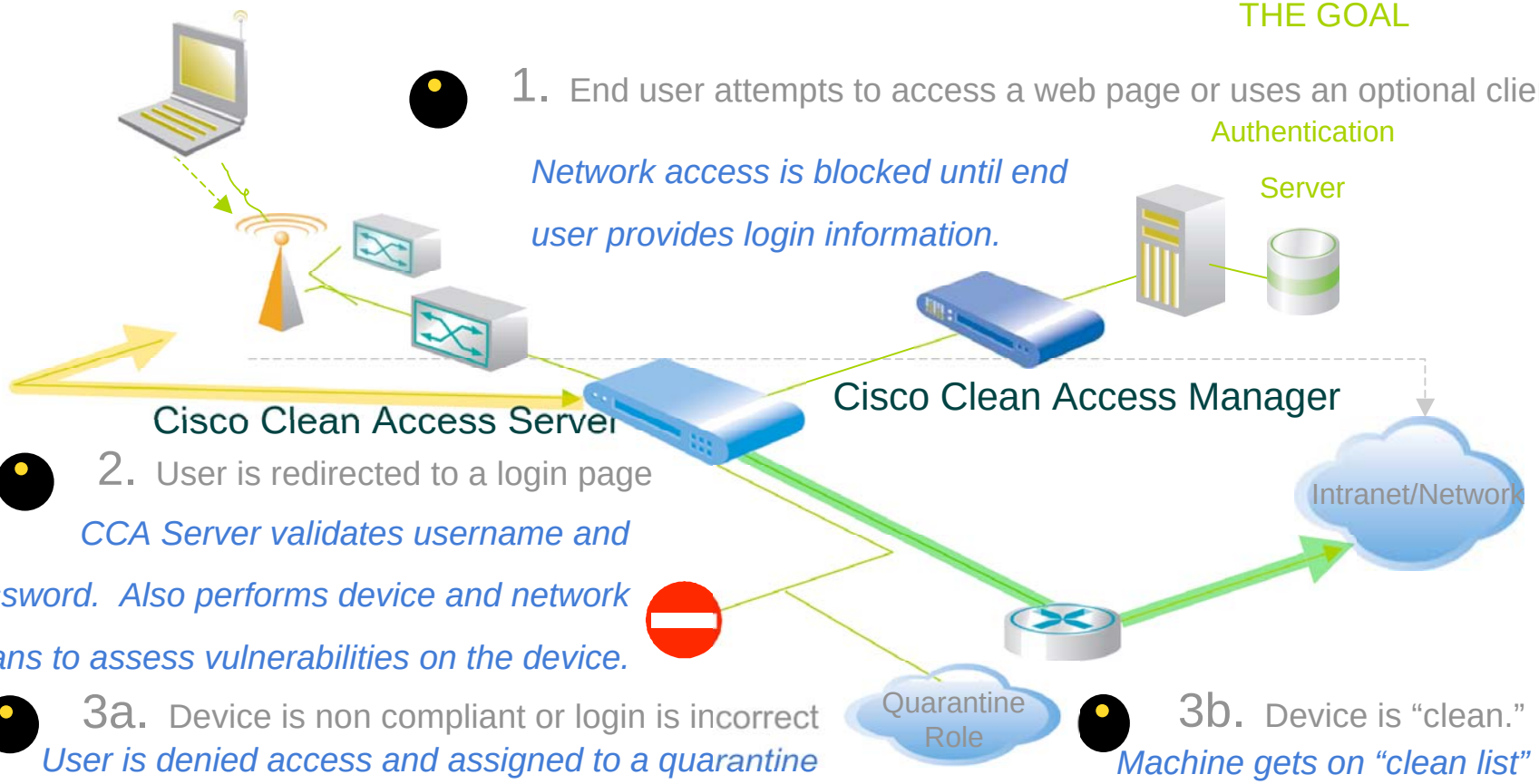
- Some NAC solutions would only mandate to prove the identity of a user using a device on the network
- Some other NAC solutions would not mandate user authentication at all, or would support NAC scenarios which user authentication will not be mandated
  - For example, with Cisco NAC Framework, two out of three operational modes do not require user authentication
- One may use a non-authorized device, with proper user credentials and introduce a rogue device onto the network…
  - In this case the consequences would be more sever (stealing a user's credentials)

© Ofir Arkin, 2006 - 2007

Validation Issues Example

Source: Cisco Clean Access presentation

Cisco Clean Access Agent (optional)



© Ofir Arkin, 2006 - 2007

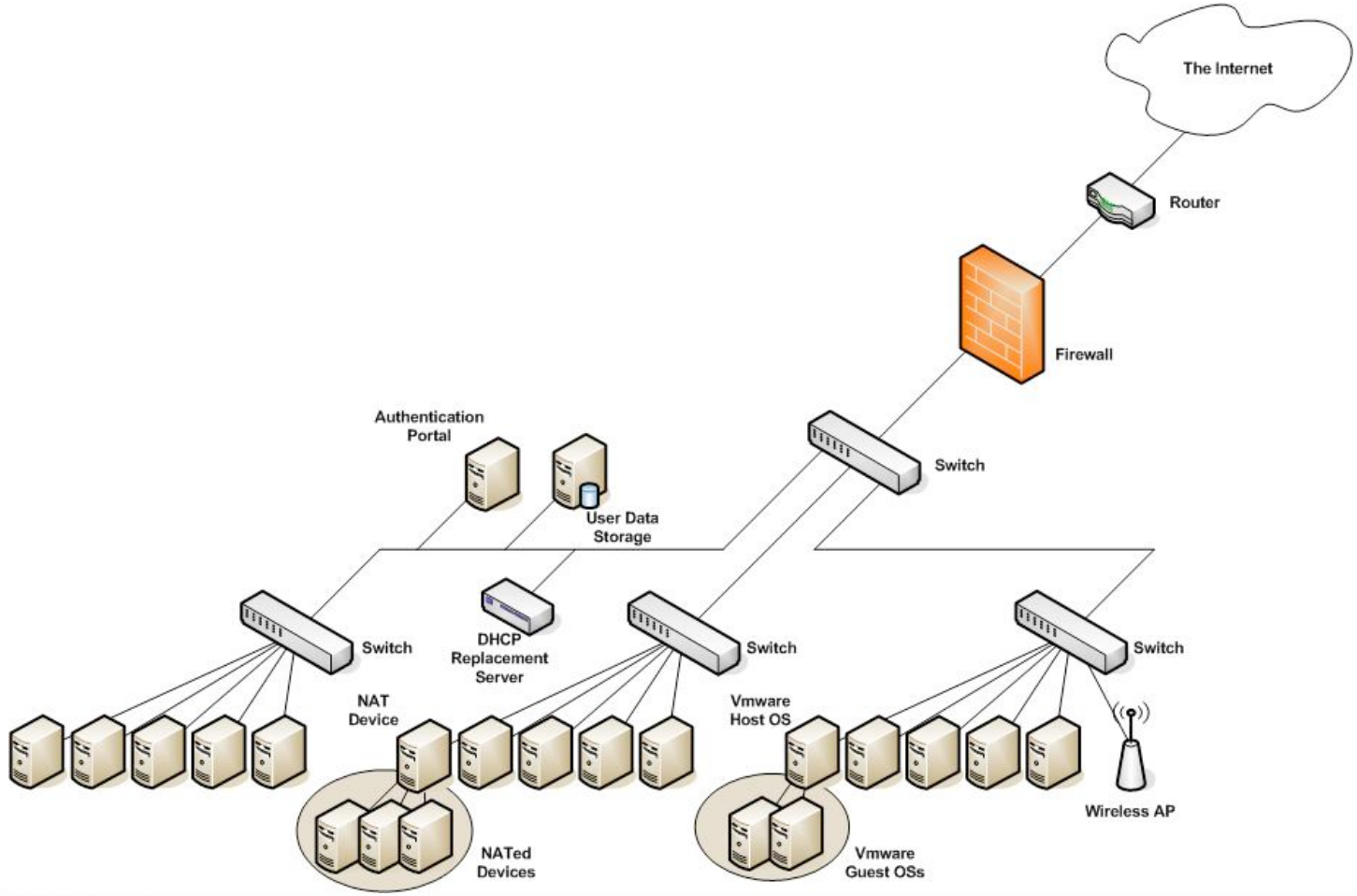
Validation

- Tying between a device and the user using the device (and its location) creates a binding which is much needed for stronger authentication, authorization, and auditing

© Ofir Arkin, 2006 - 2007

Poor User Authentication Example

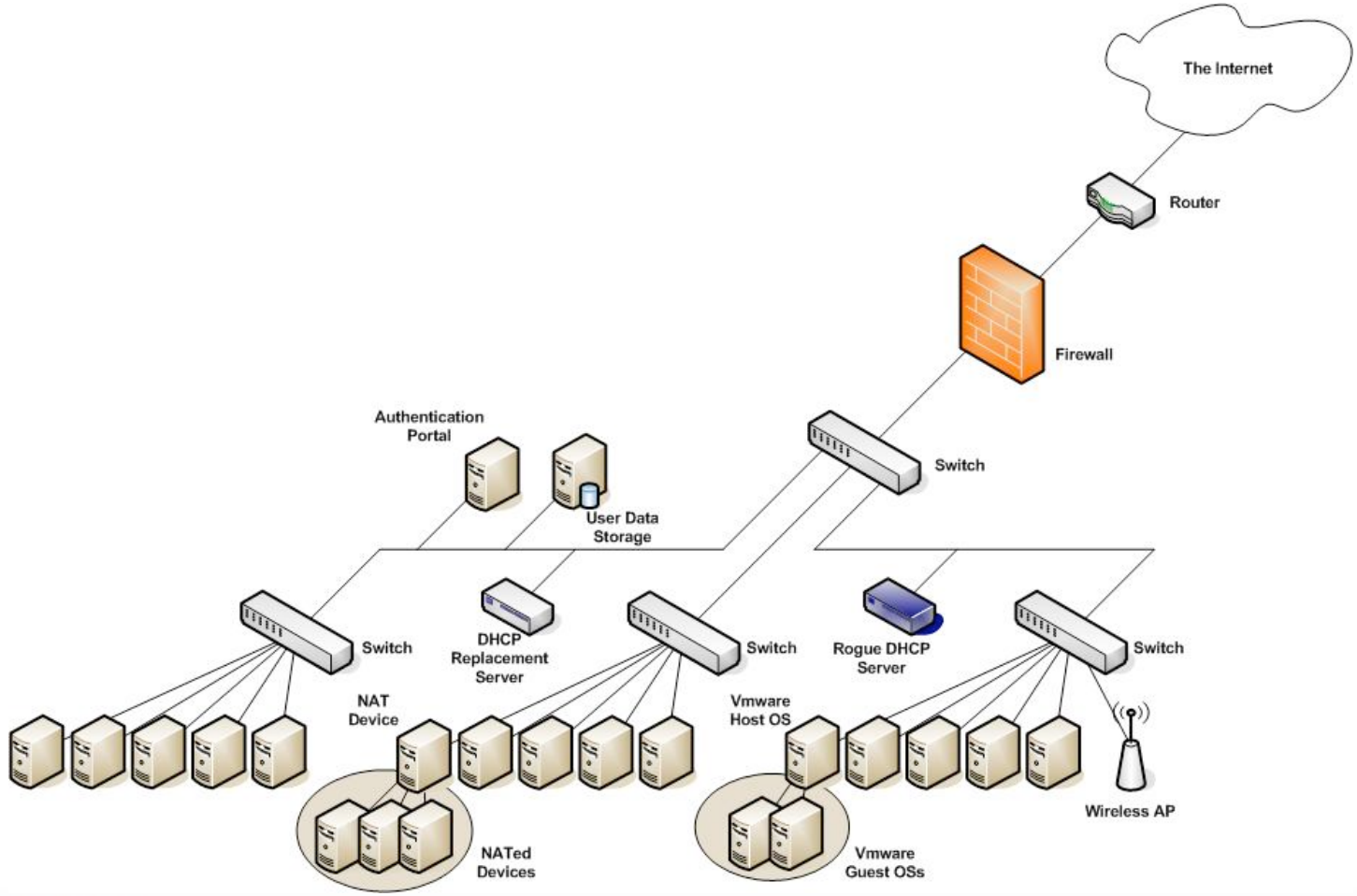
DHCP in a Box / Authenticated DHCP



© Ofir Arkin, 2006 - 2007

Poor User Authentication Example

DHCP in a Box / Authenticated DHCP



© Ofir Arkin, 2006 - 2007

A Word About 802.1x

- Just a username/password protocol and nothing more then that
  - For other capabilities a client is required
- Not a device authorization solution
  - The credentials used with 802.1x are in most cases the same as the regular username/password pair used by a user to logon to the Domain/machine

© Ofir Arkin, 2006 - 2007

Assessment

© Ofir Arkin, 2006 - 2007

Assessment

- Assessment is the process of evaluating whether an element complies with the network access policy of an organization
- Usually only Microsoft Windows-based operating systems would undergo the assessment process

© Ofir Arkin, 2006 - 2007

Device identification and classification

- A device needs to be identified and classified (OS) in order to determine whether it should, or should not, undergo the assessment process
- There are various ways to classify a device
  - Client-based software
  - Active OS detection
  - Passive OS detection
  - Java scripts on captive portals
  - Etc.

© Ofir Arkin, 2006 - 2007

Device identification and classification

- The process of classifying a device may be circumvented
  - Cisco NAC Appliance Agent Installation Bypass Vulnerability
    - http://www.securityfocus.com/archive/1/444424/30/0/threaded
    - Circumventing the 'USER-AGENT' string, manipulating the TCP/IP OS stack, enabling personal FW, etc.
  - Cisco Security Response: NAC Agent Installation Bypass
    - http://www.cisco.com/warp/public/707/cisco-sr-20060826-nac.shtml
    - "Users cannot bypass authentication using the approach described in the advisory"
  - Clean Access - Use the Network Scanning Feature to Detect Users Who Attempt to Bypass Agent Checks
    - http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080545b62.shtml (i.e. use Nessus scripts)

© Ofir Arkin, 2006 - 2007

Assessment Methods

- Client-based software
- Client-less
- Dissolving agent

© Ofir Arkin, 2006 - 2007

Agent-based

- Strengths
  - Can provide a wealth of information regarding a host
  - May detect changes in real-time

© Ofir Arkin, 2006 - 2007

Agent-based

- Weaknesses
  - Where to install the client?
    - Who are the elements we need to install this client on?
    - No contextual network information in the first place…
    - The 80/20 rule does not apply to security
  - One client among many
  - May have a performance impact
    - Try to tell IT they need to install another client on the desktop
  - Management overhead
  - Takes time to implement
  - Changing what is checked is not easy

© Ofir Arkin, 2006 - 2007

Agent-based

- Security issues
  - The first lesson in security is that one cannot trust “client-side” security measures
  - The NAC agent is a target
    - Cisco Security Advisory: Multiple Vulnerabilities in 802.1X Supplicant http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml
  - The communications between the NAC agent and its server makes another excellent venue for attack (alerted about this more then a year ago)
    - Cisco Security Response: NACATTACK Presentation http://www.cisco.com/en/US/products/products_security_response09186a00808110da.html
  - More attacks in the future will directly target NAC agents (like A/V agents are targeted today)

© Ofir Arkin, 2006 - 2007

All-In-One Agent

- An approach which preaches that a super agent which includes A/V, Anti-Spyware, personal FW, anti-SPAM, NAC, and other security features and capabilities is the best approach for NAC and end-point security
- The problem is that it is also a single point of failure
- If selectively attacked… you get the picture…

© Ofir Arkin, 2006 - 2007

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.)
  - Possible less granular information (method dependent)
  - The communications between a NAC solution and a checked device makes another excellent venue for attack

© Ofir Arkin, 2006 - 2007

Dissolving Agent

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

© Ofir Arkin, 2006 - 2007

The Information Checked

- Local
  - Some of the information which is (usually) checked (and verified) as part of an element's assessment process may be easily spoofed
  - For example, registry values of the Windows OS version, Service Pack version installed, patches installed, etc.
- Remote
  - The communications between the NAC agent and its server makes an excellent attack vector
    - Cisco Security Response: NACATTACK Presentation http://www.cisco.com/en/US/products/products_security_response09186a00808110da.html

© Ofir Arkin, 2006 - 2007

The Information Checked

- Replay attacks
  - Sniffed data of previously exchanged communications between a NAC solution to a certain client can be re-played (in a way) allowing falsifying the entire assessment process.
- S&S attack (Sniff & Spoof)
  - Sniff the communications between a NAC solution to a client in order to learn what are the parameters checked
  - Falsify the parameters/spoof the response on the checked host and get validated

© Ofir Arkin, 2006 - 2007

Exceptions

- Exceptions are defined for elements which cannot (or should not) participate in the NAC process (or part of it) for some reason
- Exceptions are defined for:
  - Elements which cannot run a certain software client
    - 802.1x
    - Non-Windows elements
  - Elements which are not running a certain operating system
    - MAC OS X
    - Linux
  - Etc.

© Ofir Arkin, 2006 - 2007

Exceptions

Source: Cisco NAC FAQ

- "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. "

© Ofir Arkin, 2006 - 2007

Cisco VoIP Devices, CDP, and NAC

- Now using NAC one can spoof CDP messages to allow a device access to the network from the Voice VLAN

© Ofir Arkin, 2006 - 2007

Exceptions

Source: Network Access Control Technologies and Sygate Compliance on Contact

- "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."

© Ofir Arkin, 2006 - 2007

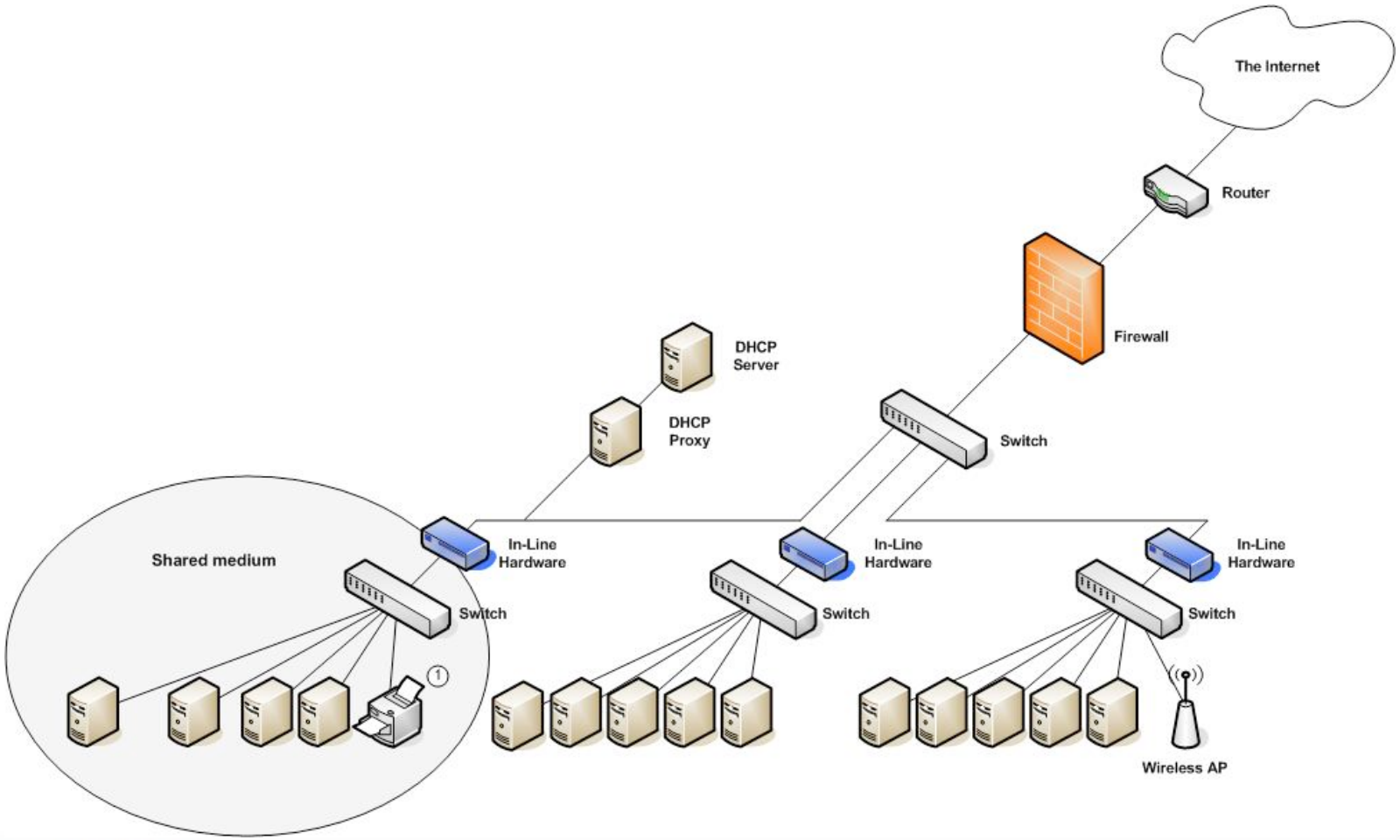
Exceptions

- In most cases NAC solutions will not have knowledge about the exception element
  - What is its operating system?
  - What is the logical location of the element?
  - What is the type of the element? (i.e. VoIP phone)
  - Does this the same element observed before?
  - Etc.
- It is possible to spoof the MAC address of a defined exception in order to receive its access rights to the enterprise LAN

© Ofir Arkin, 2006 - 2007

Bypassing Enforcement Using Exceptions

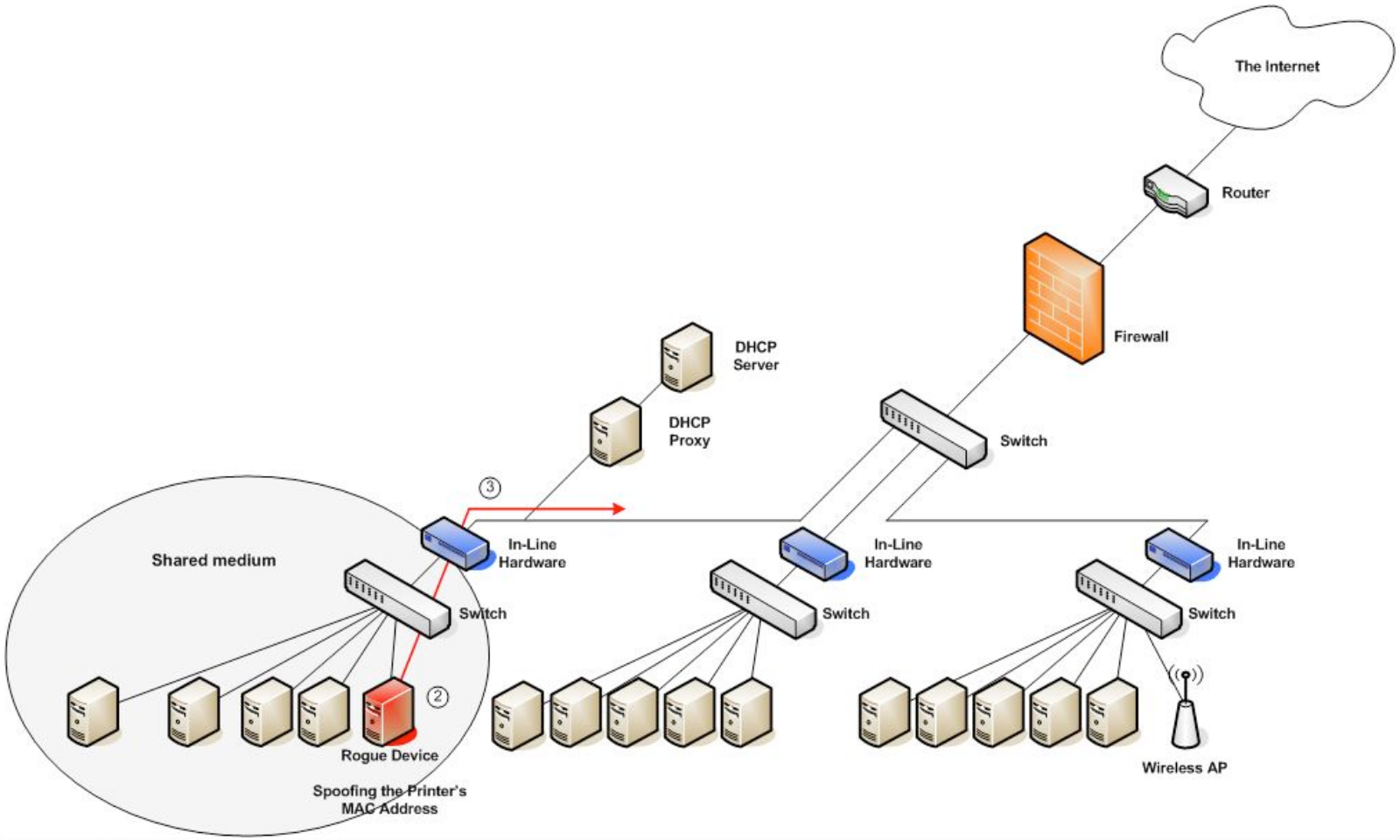
Product: Symantec (Sygate)



© Ofir Arkin, 2006 - 2007

Bypassing Enforcement Using Exceptions

Product: Symantec (Sygate)



© Ofir Arkin, 2006 - 2007

Exceptions and 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.)

© Ofir Arkin, 2006 - 2007

Exceptions and 802.1x

- Exceptions
  - Hosts that do not support 802.1x can be granted access to the network using manually configured exceptions by MAC address

© Ofir Arkin, 2006 - 2007

Quarantine

© Ofir Arkin, 2006 - 2007

Quarantine

- An element which does not comply with the network access policy will be placed into a quarantine
- The quarantine is a temporary 'holding place' for an element until the policy violation is remediated
- Access should be granted only to remediation servers
- The quarantine holds 'soft targets' that are easier to penetrate into compared to elements which comply with the network access policy

© Ofir Arkin, 2006 - 2007

Multitude Quarantine Methods

- Through the usage of ACLs on switches and/or routers
- A dedicated subnet (i.e. DHCP Proxy)
- A dedicated VLAN (i.e. The Quarantine VLAN)
- Private VLANs (PVLAN)
- Per switch port (hardware)
- Manipulating ARP cache entries at L2
- Etc.

© Ofir Arkin, 2006 - 2007

Public (Shared) Vs. Private Quarantine

- A quarantine method which allows quarantined elements to interact with each other is known as shared quarantine
- A shared quarantine makes a perfect attack vector
  - Attacking the Enterprise's 'soft targets' which are isolated and located in a single location…
  - Might also be known as the 'Self Infecting VLAN' / 'Self Infecting Subnet'

© Ofir Arkin, 2006 - 2007

Public (Shared) Vs. Private Quarantine

- Many NAC solutions uses the Quarantine VLAN method
  - Associates a device with a dedicated VLAN by dynamically assigning its VLAN ID using the switching infrastructure
    - The networking people loves this especially in controlled environments (like financial institutes) where a change request is required for any change
  - Rely on the networking infrastructure (switch) to provide with a major function of the NAC solution (quarantine)
    - What if the infrastructure is old?
  - Per-Port Per-Device policy (one to one, and not one to many)
  - Provides a shared quarantine
  - No knowledge with regards to who are the switches?
  - No knowledge with regards to who is connected where?

© Ofir Arkin, 2006 - 2007

Public (Shared) Vs. Private Quarantine

- Quarantine VLAN (Cont.)
  - No knowledge regarding the whole networking layout
    - VLAN hopping maybe possible
  - Read/Write access to the switches is required
  - VLAN tags are dynamically assigned

© Ofir Arkin, 2006 - 2007

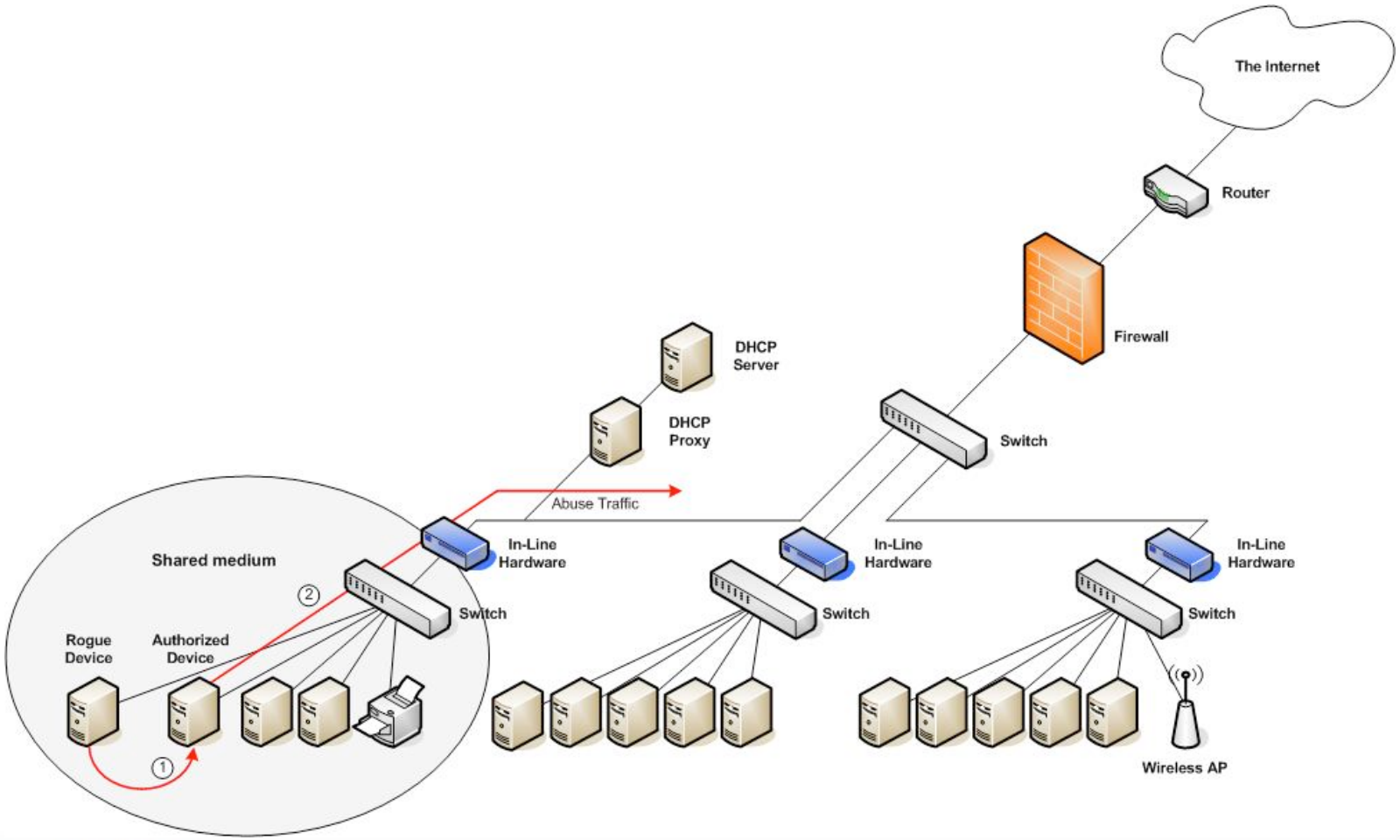
Public (Shared) Vs. Private Quarantine

- A quarantine mechanism which does not allow quarantined elements to interact with each other is known as private quarantine
- A private quarantine may be provided using:
  - Private VLANs
  - L2-based methods

© Ofir Arkin, 2006 - 2007

Layer-3 based Quarantine Bypass Example

Product: Symantec (Sygate)



© Ofir Arkin, 2006 - 2007

When should the quarantine be used?

- Only when an element should be assessed for compliance?
  - Might be too late
- After assessment, when it fails?
  - Might be too late
- Immediately when an element is introduced to the network
  - Blocking any possible interaction between the element to other elements operating on the network, as soon as a new element is introduced to the network

© Ofir Arkin, 2006 - 2007

When should the quarantine be used?

- NAC is about risk mitigation
- Real-time element detection combined with immediate quarantine closes the window of opportunity for infection and/or compromise
- But if there is no real-time element detection and/or quarantine is not done immediately, the window of opportunity is getting just bigger and bigger

© Ofir Arkin, 2006 - 2007

Enforcement

© Ofir Arkin, 2006 - 2007

Enforcement

- Enforcement is the process of blocking/restricting network access from elements which do not comply with the network access policy of an organization
- Enforcement can be performed at L3, L2 and at the switch level
- In order to provide with Enforcement additional hardware (in line devices) and/or software (agents) maybe required
- Enforcement provided at the switch level usually is done per-port per a single device
- Enforcement performed at L3 is subject to many bypass issues (i.e. assigning non-routable IP addresses, shared medium issues, etc.)

© Ofir Arkin, 2006 - 2007

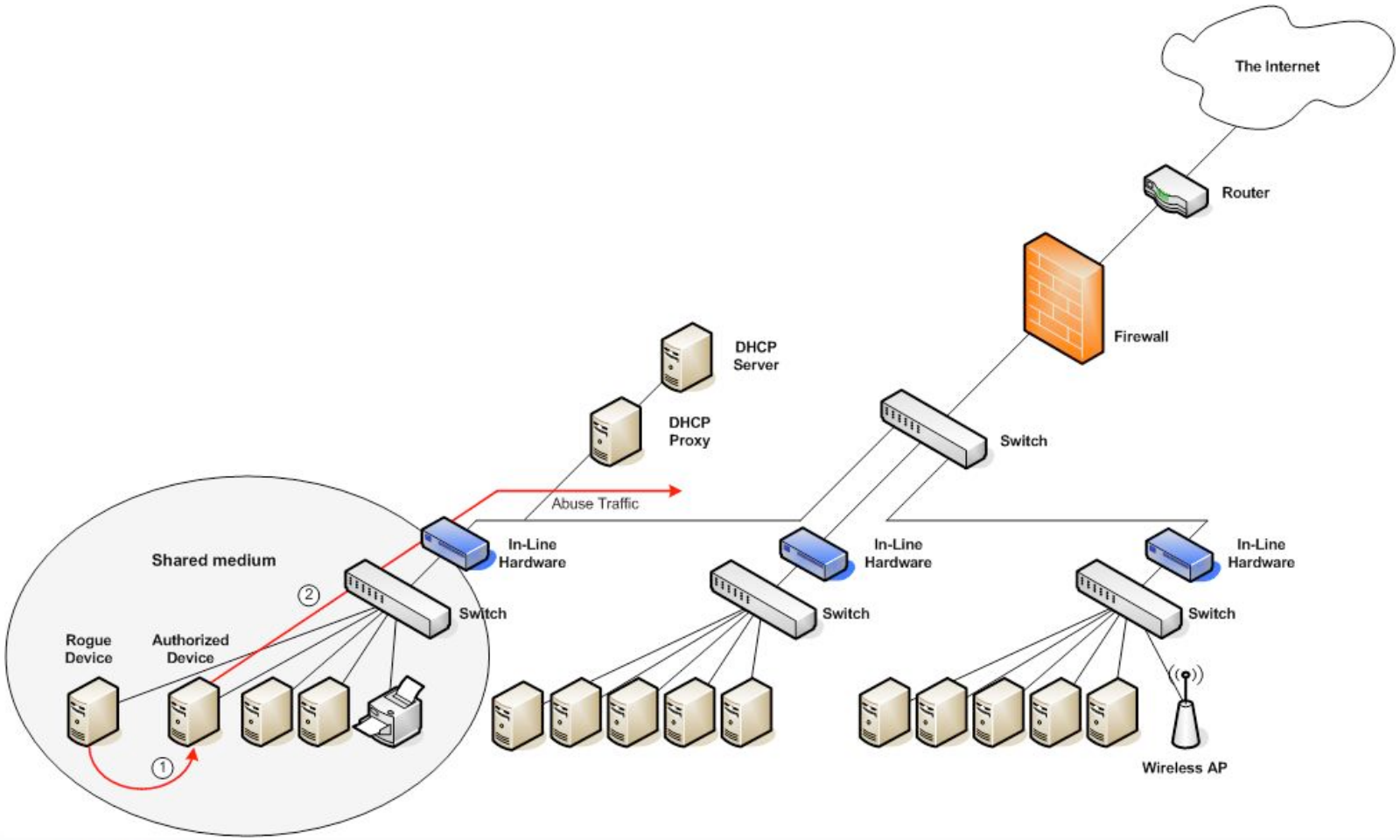
Multitude of Enforcement Methods

L3	L2	Switch
ACLs (switch/router/FW)	Manipulating ARP cache entries	802.1x
PVALNs and VACLs		Shutting down switch ports
In-line devices / GWs		
IPS Style*		

© Ofir Arkin, 2006 - 2007

Bypassing Enforcement at L3

Product: Symantec (Sygate)

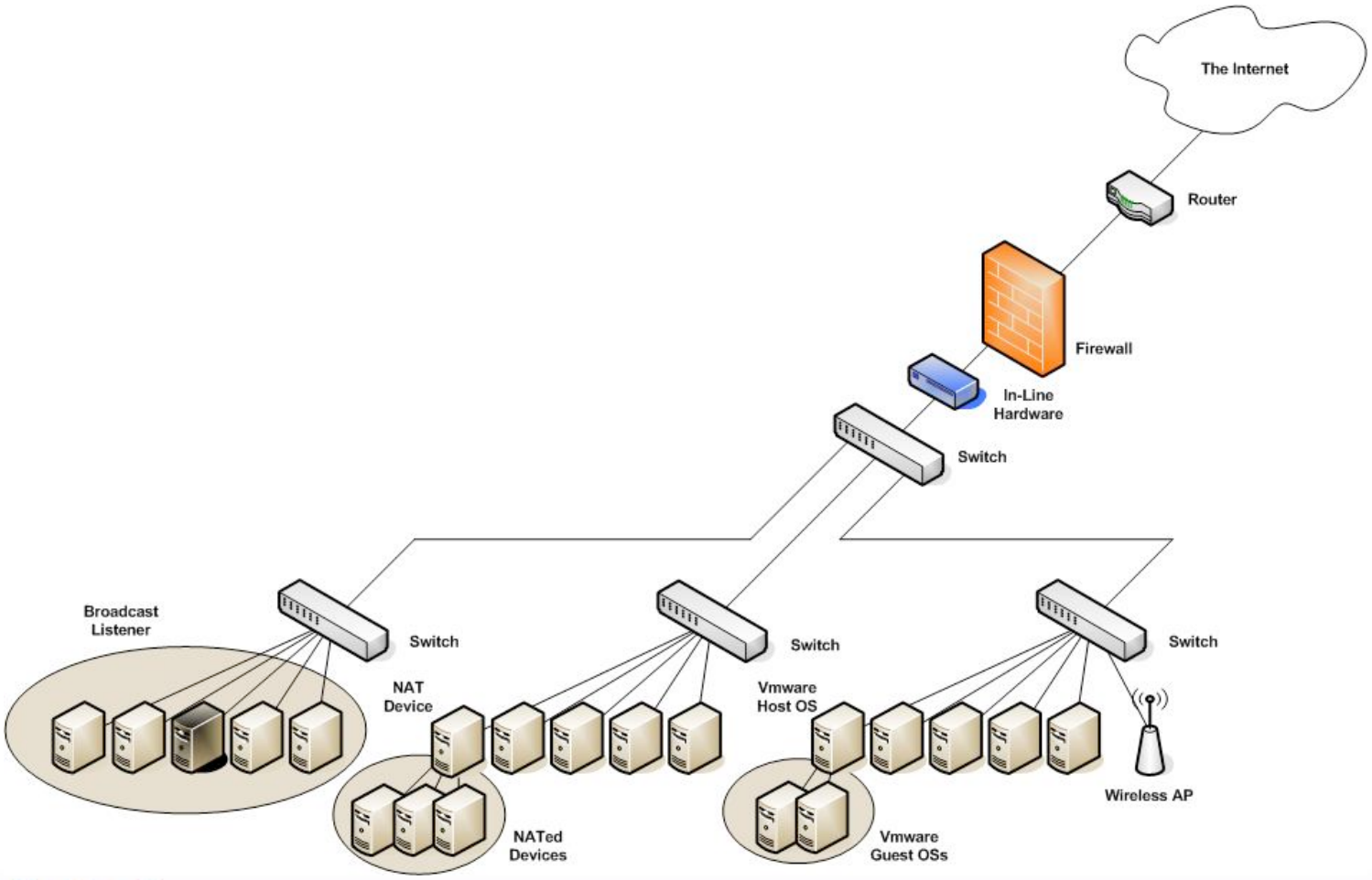


© Ofir Arkin, 2006 - 2007

Examples

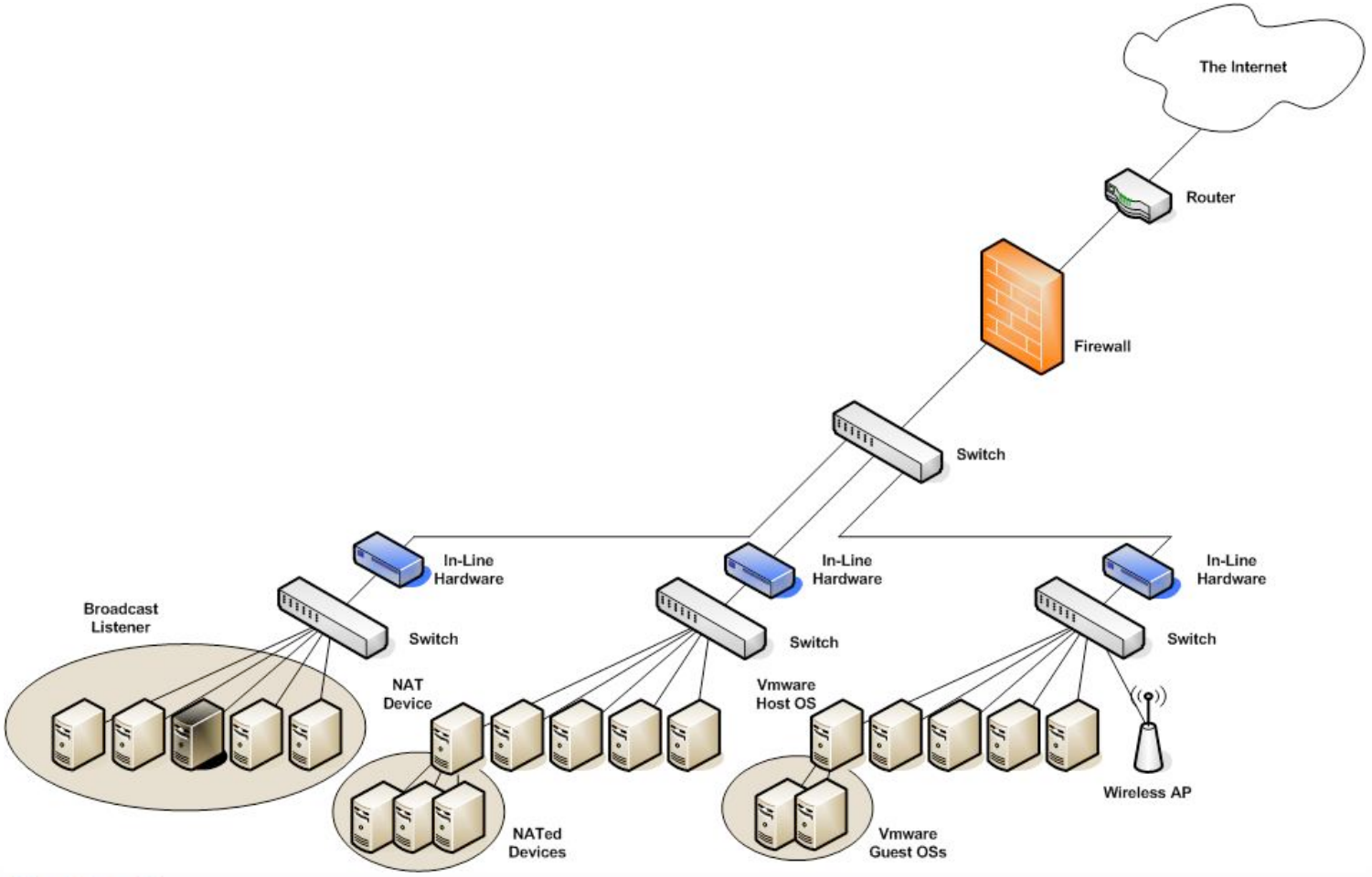
© Ofir Arkin, 2006 - 2007

Broadcast Listener & In-Line Devices Combo



© Ofir Arkin, 2006 - 2007

Broadcast Listener & In-Line Devices Combo



© Ofir Arkin, 2006 - 2007

Broadcast Listener & In-Line Devices Combo

- Deployment involves network re-architecture
- The in-line device should be deployed as close as possible to the access layer in order to be efficient
- The in-line devices is a point of failure
- Redundancy meaning 2x the cost
- The in-line device is limited by bandwidth (the more bandwidth resistance the more it costs)
- The broadcast listener must be deployed at each subnet
- One must have prior knowledge in order to fully deploy the listeners
- Cost

© Ofir Arkin, 2006 - 2007

Broadcast Listener & In-Line Devices Combo

- Element detection
  - L3 is like any other problematic L3 detection
  - L2 is like any other broadcast listener
- No form of device authorization
- No form of user authentication
- Exceptions are still needed to be used
- Quarantine using the switches
  - Shared quarantine
- The in-line device is used as an IPS. But what if the traffic is all normal and we are just accessing things we should not have to…

© Ofir Arkin, 2006 - 2007

Conclusion

© Ofir Arkin, 2006 - 2007

Conclusion

- The market place is confused
- Most of the available NAC solutions can be bypassed and do not supply with appropriate access controls
- We are starting to see a more serious attitude towards the pitfalls of various NAC solutions outlined in the ‘bypassing NAC’ original presentation
- When considering NAC know what you wish to achieve

© Ofir Arkin, 2006 - 2007

Resources

© Ofir Arkin, 2006 - 2007

Resources

- Bypassing NAC, Blackhat presentation, Ofir Arkin, 2006. Available to view at: http://www.insightix.com/resources/events/nac-presentation.aspx
- Bypassing NAC, Ofir Arkin, 2006. Available from: http://www.insightix.com/resources/whitepapers.aspx
- Risks of passive network discovery systems, Ofir Arkin, 2005. Available from: http://www.sys-security.com/blog/published-materials/papers/

© Ofir Arkin, 2006 - 2007

Questions

© Ofir Arkin, 2006 - 2007

Thank You