EASYNAC

TECHNICAL OVERVIEW

EasyNAC is a trademark of InfoExpress, Inc. Other product and service names are trademarks and service marks of their respective owners.

InfoExpress products and services are protected by one or more of the following U.S. Patents: 8347351, 8347350, 8117645, 8112788, 8108909, 8051460, 7523484, 7890658, 7590733. Additional patents pending.

www.easynac.com

v3.2.250801

CONTENTS

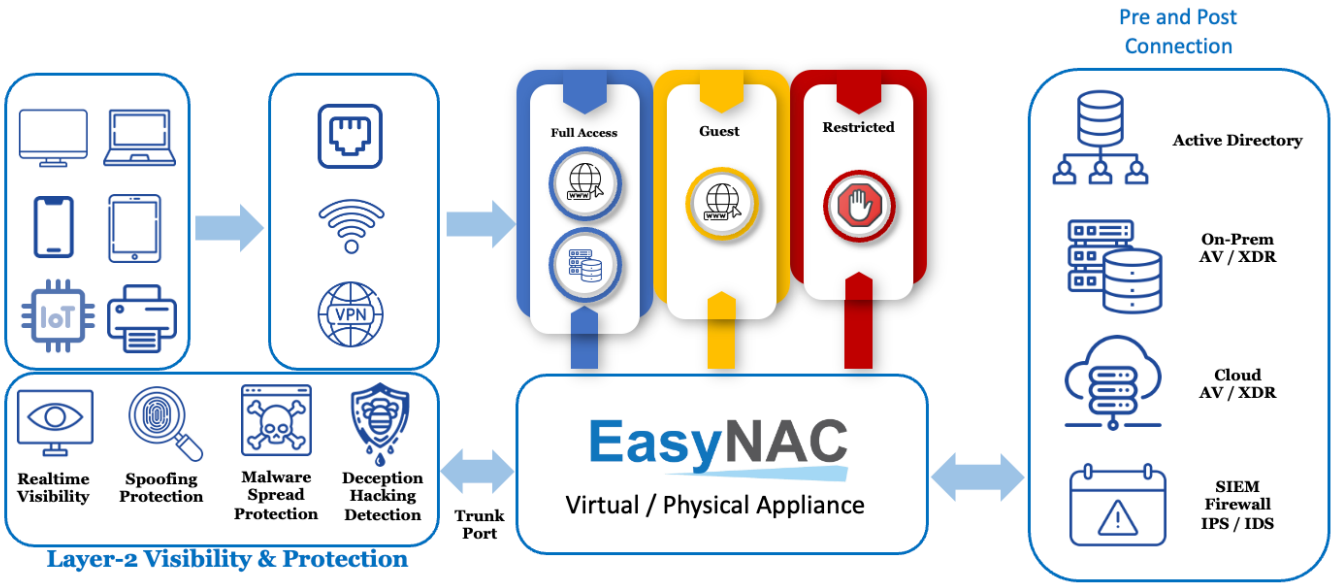
1. Overview 3
2. EasyNAC Deployment Architecture 4
3. EasyNAC Device Management Process 6
3.1 Detection – Device Discovery 6
3.2 OS Profiling – Device Profiling 7
3.3 Roles and Access Assignment – Auto Trust 9
3.4 Enforcement – Device Restriction 11
3.5 Alert - Notification 14
4. Summary 15

1. OVERVIEW

Overview

EasyNAC is an agentless network access control solution that provides strong security while being simple to deploy and manage. It utilizes a unique and innovative ARP enforcement method to offer robust network access control without requiring any changes to the existing infrastructure. This means there is no need to configure VLANs, implement 802.1x, make DHCP changes, or change the network in any way.

The EasyNAC appliances integrate seamlessly with existing cybersecurity solutions to offer additional compliance checks for managed endpoints. A single appliance can monitor and enforce security across up to 400 subnets. It effectively manages ARP information on each subnet to quarantine rogue endpoints. This is achieved through a combination of active and passive discovery of new or rogue endpoints, redirection using ARP management techniques, and filtering based on managed ACLs.



Layer-2 Visibility & Protection

The EasyNAC solution utilizes Layer-2 visibility for protection, ensuring that all devices, including computers, IoT devices, and other network-connected equipment, are monitored and secured. This visibility allows EasyNAC to enforce network policies effectively and maintain a high level of security.

Pre and Post-Connection Security and Integration to Speed Up Deployment

EasyNAC ensures robust security both before and after devices connect to the network. It performs pre-connection compliance checks and continues to monitor and enforce policies post-connection to ensure ongoing security and compliance. To accelerate the deployment process, EasyNAC can

integrate with various existing network and security infrastructures, ensuring a streamlined and efficient setup:

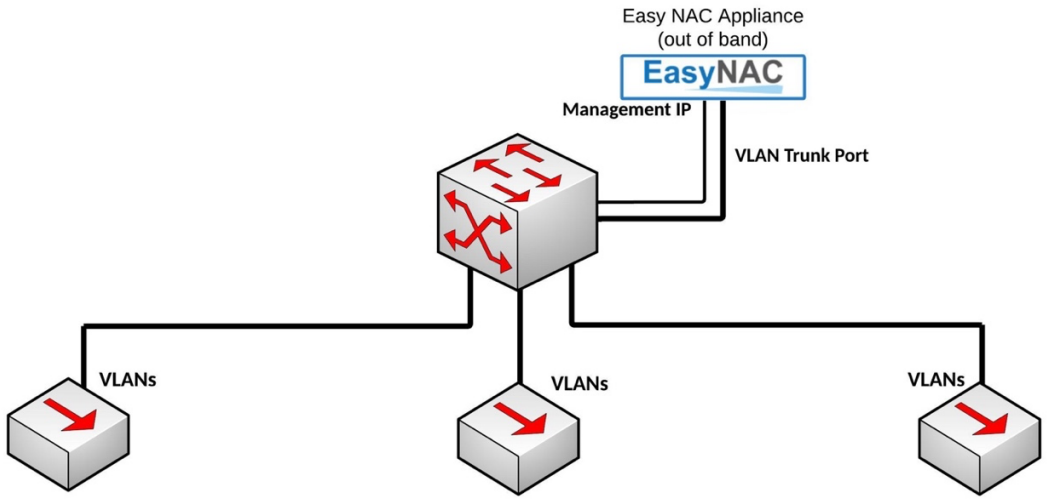
- **Active Directory (AD)**: Integration with AD allows EasyNAC to authenticate and manage devices based on existing directory information, speeding up the profiling and policy assignment processes.
- **On-Premises and Cloud-based AV/XDR Solutions**: Integration with Antivirus (AV), Endpoint Detection & Response (EDR) solutions and Extended Detection and Response (XDR) solutions, both on-premises and cloud-based, helps in maintaining endpoint compliance and enhancing threat detection capabilities.
- **Patch Management Systems**: Integration with patch management systems ensures that all devices are up to date with the latest security patches, reducing vulnerabilities and improving overall network security.
- **Desktop Management Systems**: EasyNAC can work with desktop management systems to enforce compliance and security policies on endpoint devices, ensuring consistent security posture across all managed desktops.

2. EASYNAC DEPLOYMENT ARCHITECTURE

EasyNAC appliances can be set up anywhere there is Layer 2 connectivity to protect different subnets. Here are three easy ways to connect a subnet to a EasyNAC appliance:

- **Method 1 – Physical connection**: Simply add an extra network adapter and plug it into a switch access port. This lets you protect an additional subnet.

- **Method 2 – 802.1q trunk**: Use 802.1q trunk ports so multiple VLANs can be protected with a single ethernet adapter. Multiple adapters are recommended if there is extensive traffic from devices being restricted with ACLs.

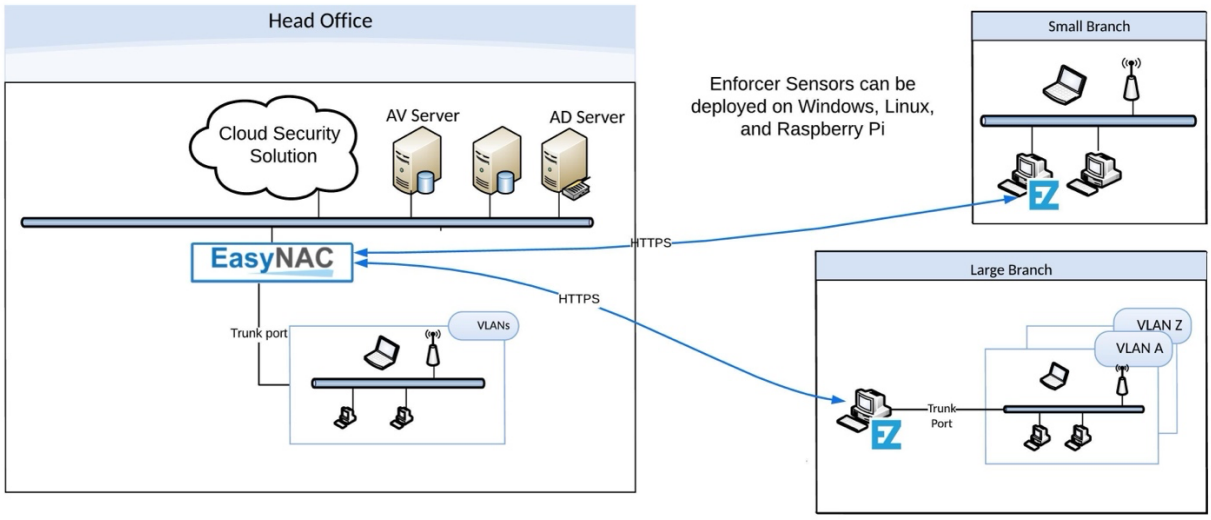


If there are remote locations and Layer-2 traffic cannot be trunked back to the EasyNAC appliance, then a separate EasyNAC appliance can be deployed at each of the remote sites. A Central Visibility Manager can be used to manage these multiple appliances.

For smaller remote sites, Method 3 below provides an economical way to deploy EasyNAC.

- **Method 3 – Enforcer Sensor or vLinks for Remote Sites**: The EasyNAC appliance needs to see all the Layer 2 traffic in the subnets it's protecting. At the main site, this can be done using trunk ports or standard access ports. However, for remote sites there are two options to bring layer 2 visibility back to the EasyNAC appliance.
    - **Enforcer Sensor**: Install Enforcer Sensors, which is a software solution that can be deployed on Windows, Linux, and Raspberry Pi hardware. These sensors work over SSL to send traffic back to the EasyNAC appliance.
    - **vLinks**: A dedicated 5-port hardware box that tunnels Layer 2 traffic back to a central vLinks appliance directly connected to the EasyNAC appliance. The tunnel is built through your existing Layer 3 VPN or MPLS network.

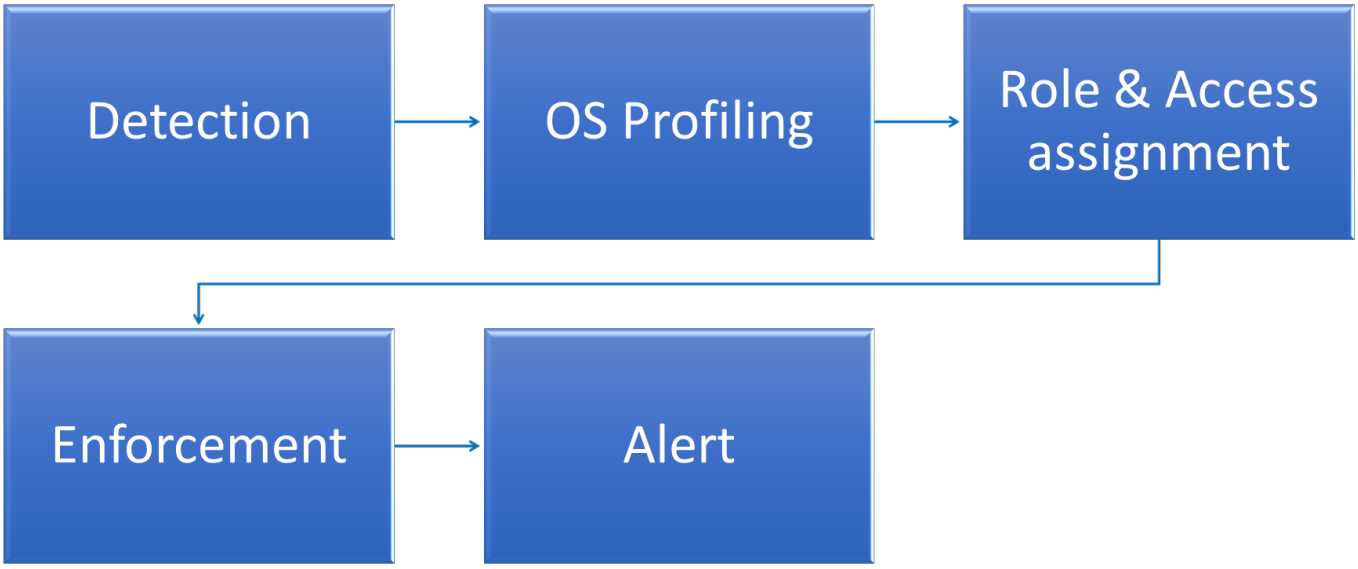
Enforcer Sensors are typically the recommended solution designed to extend the reach of EasyNAC appliances to protect remote sites with affordable software and hardware options. At Remote Sites, simply deploy an Enforcer Sensor on the network with an IP address. Enforcer Sensors will then send layer 2 traffic over SSL directly to the EasyNAC appliance.



All EasyNAC features, including compliance checks, captive portals, and Automated Threat Response, are supported with this configuration. This ensures that your network is secure and compliant across both main and remote sites.

3. EASYNAC DEVICE MANAGEMENT PROCESS

The following diagram outlines the step-by-step process that EasyNAC uses to manage devices on a network, ensuring robust security and compliance from the moment a device connects to the network through to enforcement and alerting. Each of these steps will be discussed in detail in subsequent sections.



3.1 DETECTION – DEVICE DISCOVERY

EasyNAC uses a combination of active and passive detection mechanisms to discover new endpoints when they join the network. This ensures that all devices, whether they use DHCP or static IP addresses, are accurately identified and monitored.

DHCP Devices

- **DHCP DISCOVER Requests:** When a new device connects to the network using DHCP, it sends out a DHCP DISCOVER request to find a DHCP server. This broadcast packet is visible to all devices on the same subnet, including the EasyNAC appliance.
- **ARP Requests:** Once an IP address is assigned by the DHCP server, the device will send out ARP requests to learn the MAC address of an IP address. The EasyNAC appliance captures these ARP requests to confirm the presence and identity of the new device.

Static IP Address Devices

- **ARP Requests:** Devices with static IP addresses do not broadcast DHCP requests. Instead, they send out ARP requests, which are broadcast traffic, to communicate with other devices on the network. The EasyNAC appliance listens for these ARP requests to detect these devices.

- **Periodic Network Scanning**: To identify devices that might be stealthily connected to the network without sending frequent ARP requests, the EasyNAC appliance performs periodic network scans. These scans ensure that even devices with minimal network activity are detected and monitored.

  PS. For large subnets, such as Class B or above, scanning the entire address space may not be practical and can increase workload. Therefore, network scanning is disabled by default for these larger subnets. Despite this, disabling network scanning does not compromise security or the effectiveness of device detection.

3.2 OS PROFILING – DEVICE PROFILING

Once EasyNAC detects a new device on the network, it proceeds to profile the device to gather detailed information about its operating system and other attributes such as open ports. This step is crucial for determining the operating system of each device and for making informed decisions about access control. The profiling process combines both passive and active techniques:

Passive Profiling

Passive profiling involves listening to network traffic generated by the device without actively probing it. The main techniques include:

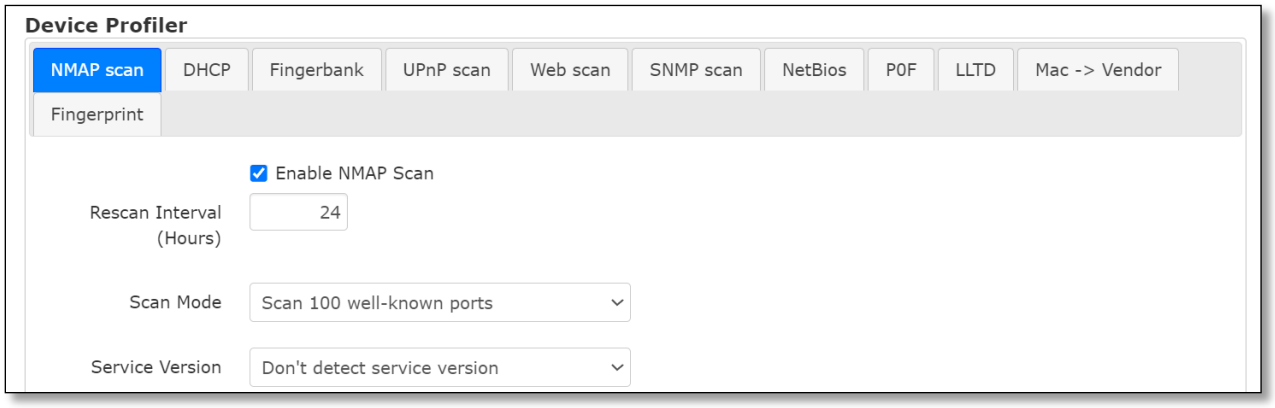
- **DHCP Fingerprinting**: When a device sends out a DHCP DISCOVER request, EasyNAC captures this packet and compares it to a database of known DHCP fingerprints to identify the operating system and other characteristics of the device.
- **HTTP Agent Access**: By analyzing HTTP headers when a device accesses web resources such as captive portal, EasyNAC can gather identifying information about the device, such as the operating system and browser type.
- **P0f Fingerprinting**: P0f (Passive OS Fingerprinting) analyzes the TCP/IP stack of the device by examining packets it sends to EasyNAC. This helps determine the operating system and other attributes without sending any active probes.
- **Integration Modules**: EasyNAC reads from integration backend servers to collect additional data about the device. This can include information from Active Directory, endpoint security solutions, enhancing the accuracy of the device profile.

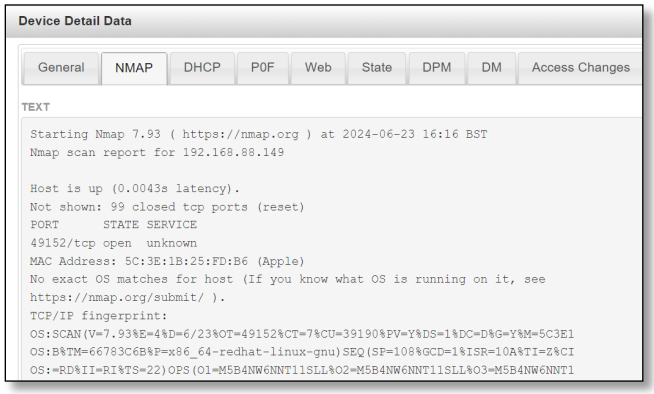
Active Profiling

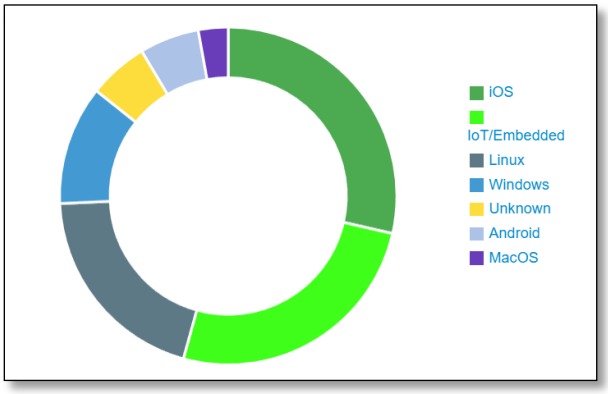
Active profiling involves sending probes and scans to the device to gather information. The primary methods used include:

- **NMAP Scans**: NMAP is used to perform comprehensive scans that identify the operating system, open ports, and services running on the device. This helps in understanding the operating system and attributes of the device (such as open ports).

- **uPnP Scans:** Universal Plug and Play (uPnP) scans read device information via the uPnP protocol, providing details about the device's capabilities and services.
- **Windows RDP Scans:** For devices running Windows, EasyNAC can connect to the Remote Desktop Protocol (RDP) port to collect information about the device.
- **SNMP Scans:** Simple Network Management Protocol (SNMP) scans are used to query network switches for detailed information about devices connected to it.
- **WMI Scans:** Windows Management Instrumentation (WMI) scans are used to gather system information from Windows-based devices by querying the WMI interface.







3.3 ROLES AND ACCESS ASSIGNMENT – AUTO TRUST

After EasyNAC profiles a device to determine its operating system and open ports, it moves on to the role and access assignment phase. This phase is critical for enforcing network access policies and ensuring that each device has the appropriate level of access based on its compliance status and role within the organization.

Auto Trust Policy

EasyNAC uses predefined policies to automatically assign roles to devices based on the profiling information gathered. The roles determine the level of network access and permissions granted to each device.

Auto Trust Policy

Activate | Cancel Changes

Add Rule

Conditions	Actions taken when conditions are met	
Device is on routerlist	Set role to full-access - Device is on routerlist	
Device is on allowlist	Set role to full-access - Device is on allowlist	
Device is on blocklist	Set role to restricted - Device is on blocklist	
Deception Event - Honey Pot hit detected Has all of these tags: Deception-Event, Honeypot-hit	Set role to High-Risk-Event - Suspicious behavior detected Send message to: Admin via Email	
Fingerprint Mismatch Has any of these tags: FP-mismatched	Set role to High-Risk-Event - Device failed fingerprint check	
Malware Lateral Spread Risk - Scan Detected Has all of these tags: Dark-IP-scan, Scan-detected	Set role to High-Risk-Event - Excessive network scanning activity was detected	
Orchestration Event Has any of these tags: SIEM-Event, IPS-Event, infected, FW-Event, APT-Event	Set role to High-Risk-Event - Malware or suspicious behavior has been detected	
Passed Agent Audit Passed Agent Audit	Set role to full-access - Passed agent audit	
Failed Agent Audit Failed Agent Audit	Set role to failed-agent-audit - Failed agent audit	
Endpoint Security Non-Compliance (agent-less checks) Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant - Device is NOT compliant with the corporate endpoint security policy	
Patch Non-Compliance (agent-less checks) Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant - Device is NOT compliant with the corporate patch management policy	
Trusted Managed Device Has any of these tags: AD-managed, AV-managed, enforcer, managed-device, patch-managed, XDR-managed	Set role to full-access - Assigned trusted managed device tag	
Trusted IOT Device Has any of these tags: enforcer, network-infrastructure, printer, switch, VoIP	Set role to full-access - Assigned trusted IOT device tag	
BYOD Registration Has any of these tags: byod	Set role to BYOD - Device registered with authorized credentials	
Consultant Registration Has any of these tags: consultant	Set role to consultant - Device registered as consultant	
Guest Registration Completed Guest or Device Registration	Set role to guest - Device registered by guest	

Note: If none of the above conditions are met, a device will be assigned to the Untrusted Role

EasyNAC enforces a Zero Trust security model. If a device does not meet any criteria specified in the auto trust policy, it is deemed unauthorized and assigned an "untrusted" role. As a result, EasyNAC quarantines the device, restricting its network access to protect the network from potential threats.

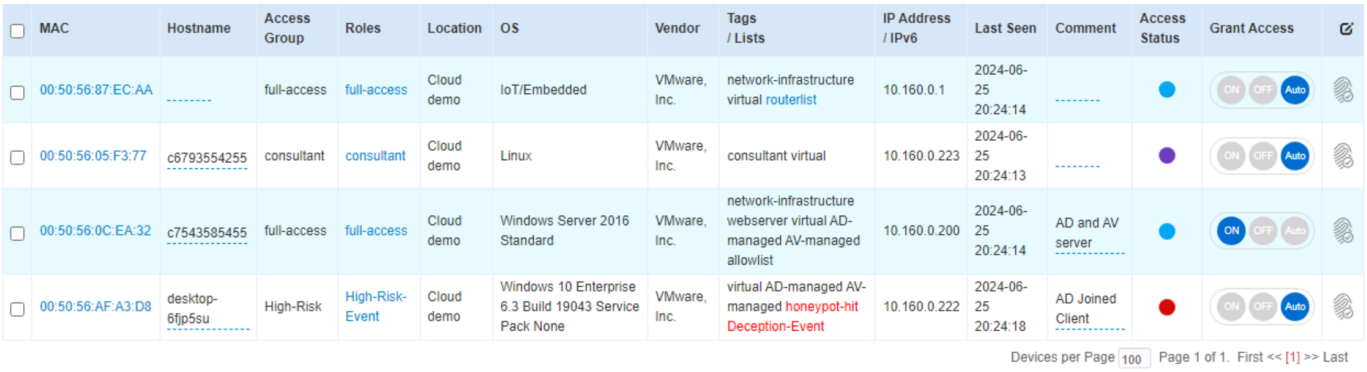
Policy Conditions

EasyNAC uses various conditions to determine which role to assign to a device. These conditions are based on data collected during the profiling process, such as:

- **Operating System**: The type and version of the operating system can influence the assigned role, especially if certain OS versions are deemed more secure or vulnerable.
- **Compliance Status**: Integration with systems like Active Directory, antivirus solutions, and patch management systems allows EasyNAC to check the compliance status of each device. Devices that meet all compliance criteria are typically granted higher access levels.
- **Device Type**: The type of device, such as BYOD (Bring Your Own Device), guest access devices, or corporate-owned devices, can influence its role assignment. For example, corporate devices are typically granted higher access levels compared to BYOD and guest devices, which often have more restricted access to ensure network security.
- **Security Posture**: The overall security posture is determined by factors such as malware lateral spread detection, honeypot deception, and other advanced security measures. Devices exhibiting suspicious behavior or known vulnerabilities are more likely to receive restricted access.

Dynamic Role Adjustment

EasyNAC continuously monitors devices and can dynamically adjust their roles based on real-time changes in their status. For example, if a device that was initially compliant becomes non-compliant (e.g., due to a security posture violation), EasyNAC can automatically restrict its access. Conversely, once the issues are resolved, the device's access can be allowed. This dynamic adjustment ensures that network security is always maintained.



MAC	Hostname	Access Group	Roles	Location	OS	Vendor	Tags / Lists	IP Address / IPv6	Last Seen	Comment	Access Status	Grant Access
00:50:56:87:EC:AA	--------	full-access	full-access	Cloud demo	IoT/Embedded	VMware, Inc.	network-infrastructure virtual routerlist	10.160.0.1	2024-06-25 20:24:14	--------		ON OFF Auto
00:50:56:05:F3:77	c6793554255	consultant	consultant	Cloud demo	Linux	VMware, Inc.	consultant virtual	10.160.0.223	2024-06-25 20:24:13	--------		ON OFF Auto
00:50:56:0C:EA:32	c7543585455	full-access	full-access	Cloud demo	Windows Server 2016 Standard	VMware, Inc.	network-infrastructure webserver virtual AD-managed AV-managed allowlist	10.160.0.200	2024-06-25 20:24:14	AD and AV server		ON OFF Auto
00:50:56:AF:A3:D8	desktop-6fjp5su	High-Risk	High-Risk-Event	Cloud demo	Windows 10 Enterprise 6.3 Build 19043 Service Pack None	VMware, Inc.	virtual AD-managed AV-managed honeypot-hit Deception-Event	10.160.0.222	2024-06-25 20:24:18	AD Joined Client		ON OFF Auto

Devices per Page 100 Page 1 of 1. First << [1] >> Last

Access Control Lists (ACLs)

The assigned roles are enforced using Access Control Lists (ACLs), which define the specific network permissions and restrictions for each role. ACLs ensure that devices can only access the resources authorized, based on their assigned role.

3.4 ENFORCEMENT – DEVICE RESTRICTION

EasyNAC uses ARP Enforcement to provide network access control functionality without requiring any changes to the existing network infrastructure. ARP, or Address Resolution Protocol, is a basic and well-understood TCP/IP standard. EasyNAC leverages ARP in a way that does not interfere with other authorized devices on the network.

How ARP Enforcement Works

- **Detection and Initial ARP Reply:** When an unauthorized device is detected, the EasyNAC appliance will automatically and regularly send out ARP REPLY packets to update the ARP table of the unauthorized device whenever it attempts to communicate. This process ensures that any device the rogue device tries to communicate with will also have its ARP table updated to prevent communication with the rogue device.

- **Traffic Diversion:** As a result of these ARP REPLY packets, traffic to and from the unauthorized device is diverted through the EasyNAC appliance. This immediate action restricts the network access of the untrusted device. An Access Control List (ACL) can be configured so the appliance will only forward packets permitted by the assigned ACL.

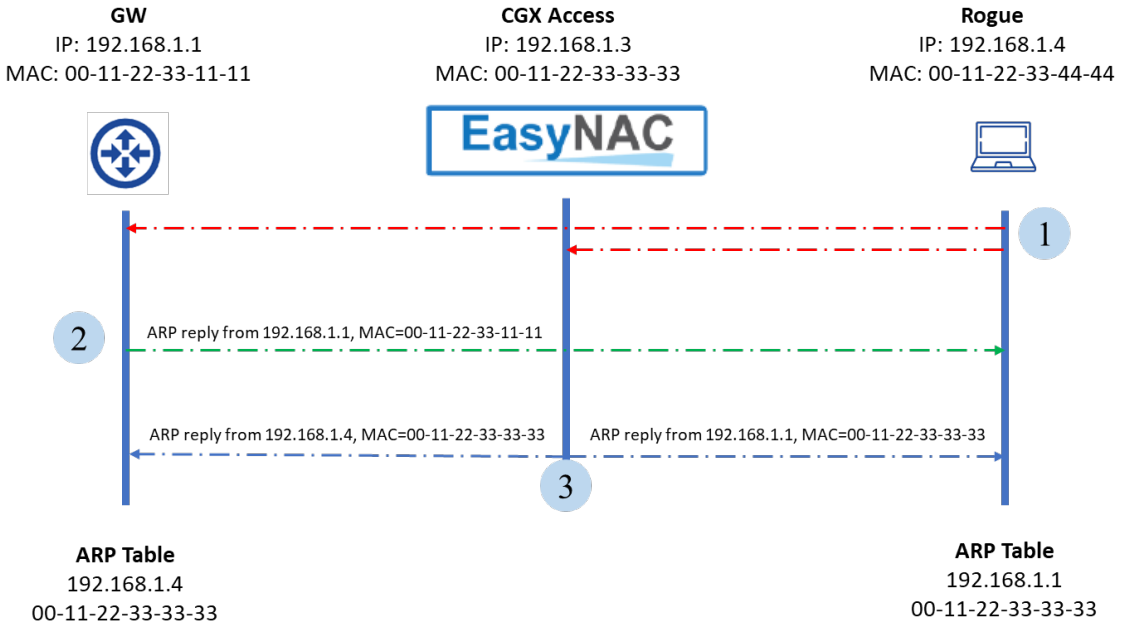
- **Directed ARP REPLY:** EasyNAC uses directed ARP REPLY packets rather than ARP BROADCAST. This approach ensures that only unauthorized endpoints are redirected via ARP without introducing unnecessary traffic to the network. Authorized endpoints continue to use the network without experiencing any slowness or delay in network performance.

- **Bypassing Static ARP Entries:** Unauthorized endpoints cannot bypass this enforcement mechanism using static ARP entries. EasyNAC will still monitor the attempted communication and send ARP updates to the devices the rogue endpoint tries to reach.

- **Guest and BYOD Access:** For guest or BYOD devices, the ACL can be configured to redirect any HTTP traffic to the EasyNAC captive portal for BYOD or guest access registration.

Enforcement by example

The following diagram illustrates the process of device detection and enforcement using EasyNAC.



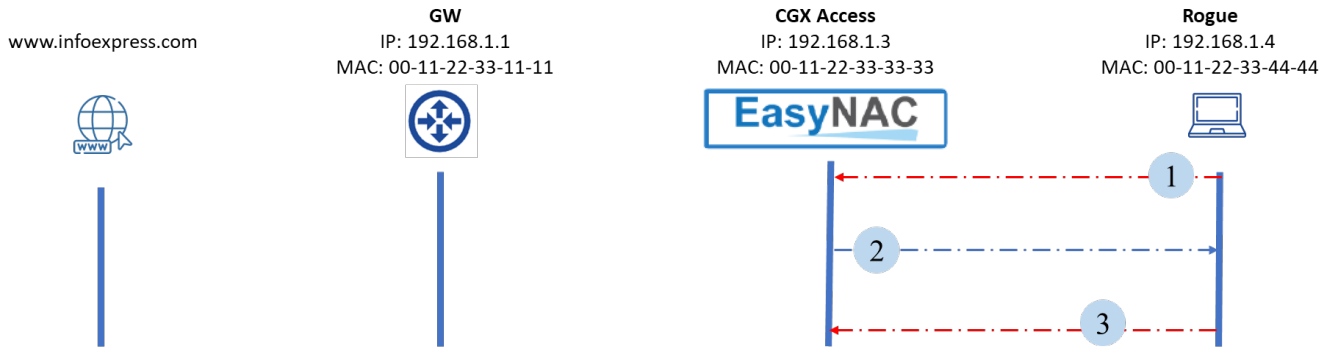
1. **Initial ARP Broadcast:**
   - The rogue device (IP: 192.168.1.4, MAC: 00-11-22-33-44-44) connects to the network and sends out an ARP broadcast to learn the MAC address of the gateway (GW) (IP: 192.168.1.1, MAC: 00-11-22-33-11-11).
   - This ARP broadcast packet can reach all devices within the same subnet/VLAN.
2. **Gateway Response:**
   - Upon receiving the ARP request from the rogue device, the GW replies with its MAC address (00-11-22-33-11-11) via an ARP reply packet.
3. **EasyNAC Detection:**
   - The EasyNAC appliance (IP: 192.168.1.3, MAC: 00-11-22-33-33-33) also receives the ARP broadcast sent by the rogue device. This allows EasyNAC to detect the rogue device.
   - Once EasyNAC confirms that this rogue device should be restricted, it sends out two ARP reply packets:
     - One ARP packet to the router impersonates the rogue, so the router updates its ARP table to think the rogue's IP (192.168.1.4) is associated with EasyNAC's MAC address (00-11-22-33-33-33).
     - Another ARP packet to the rogue impersonates the router, so the rogue updates its ARP table to think the router's IP (192.168.1.1) is associated with EasyNAC's MAC address (00-11-22-33-33-33).

- EasyNAC continually sends these ARP packets to ensure that the rogue device's ARP table always points to EasyNAC for other IP addresses, maintaining the restriction.

4. **Traffic Control**:
   - From this point forward, any traffic sent from the rogue device to the router is "captured" by the EasyNAC appliance. This diversion of traffic allows EasyNAC to enforce network policies and apply Access Control Lists (ACLs) to the traffic from the rogue device.

Redirection by example

The following diagram illustrates the process of redirecting a rogue device to a captive portal using DNS replies, managed by the EasyNAC appliance.



1. **Initial Access Attempt**:
   - The rogue device (IP: 192.168.1.4, MAC: 00-11-22-33-44-44) tries to access the website www.infoexpress.com via a web browser. Since the traffic has been captured by EasyNAC (IP: 192.168.1.3, MAC: 00-11-22-33-33-33), the request is sent to EasyNAC instead of the gateway (IP: 192.168.1.1, MAC: 00-11-22-33-11-11).
2. **ACL Comparison and DNS Reply**:
   - EasyNAC compares the request against the configured Access Control List (ACL) to determine if the traffic should be allowed. If the ACL includes a DNSREPLY rule, EasyNAC can directly respond with the IP address configured for the redirection without needing to query a DNS server.
3. **Redirection**:
   - The rogue device receives the DNS reply packets from EasyNAC. Following the IP address provided in the redirection ACL, the rogue device is redirected to the specified IP, typically a captive portal for BYOD or guest access registration.

3.5 ALERT - NOTIFICATION

EasyNAC provides a robust alerting system to ensure that NAC administrators are promptly informed about significant events, policy violations, and potential security threats. These alerts help in maintaining real-time awareness of network activities and enable swift response to any issues. EasyNAC supports multiple channels for delivering these alerts, ensuring flexibility and reliability.

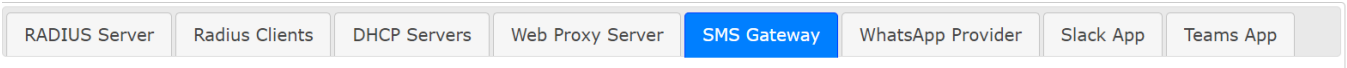
Types of Alerts

- **Policy Violations**: Alerts triggered when a device violates network policies or fails to comply with security standards.
- **Unauthorized Access**: Notifications sent when an untrusted or rogue device attempts to access restricted network resources.
- **Compliance Issues**: Alerts generated when a device fails to meet compliance requirements, such as missing patches or outdated antivirus definitions.
- **Security Incidents**: Immediate notifications for detected security threats, such as malware detection, lateral movement attempts, or network anomalies.

Alert Channels

EasyNAC supports a variety of channels for sending alerts, ensuring that NAC administrators can receive notifications through their preferred communication methods:

- **Email**: Detailed alerts sent via email, providing comprehensive information about the event, including the affected device, nature of the alert, and recommended actions.
- **SMS**: Short Message Service (SMS) alerts for critical events, ensuring that administrators receive immediate notifications even when they are away from their computers.
- **WhatsApp**: Alerts sent via WhatsApp for quick and convenient notifications, allowing administrators to stay informed through a commonly used messaging platform.
- **Teams**: Integration with Microsoft Teams to send alerts directly to team channels or individual users, facilitating collaboration and immediate response.
- **Slack**: Alerts delivered to Slack channels, enabling real-time communication and collaboration among IT and security teams.
- **Syslog**: Alerts logged via Syslog for integration with other monitoring and logging systems, helping to centralize alert management and analysis.



4. SUMMARY

EasyNAC is a comprehensive, agentless network access control solution designed to provide robust security while being simple to deploy and manage. By leveraging a unique ARP enforcement method, EasyNAC offers powerful network access control without the need for changes to existing infrastructure. It ensures Layer-2 visibility and protection, enabling effective monitoring and security for all devices, including computers, IoT devices, and other network-connected equipment.

EasyNAC's deployment architecture is flexible, supporting physical connections, 802.1q trunk ports, and remote site configurations using Enforcer Sensors or vLinks appliances. This flexibility allows for seamless integration into various network environments, ensuring that even remote and cost-sensitive locations are secured.

The EasyNAC device management process encompasses detection, profiling, role and access assignment, enforcement, and alerting. EasyNAC uses a combination of active and passive detection mechanisms to identify devices accurately. It profiles devices to gather detailed information about their operating systems and open ports, using both passive techniques (like DHCP fingerprinting and HTTP agent access) and active techniques (such as NMAP and SNMP scans).

Roles and access are assigned based on predefined policies and real-time monitoring. The system enforces a Zero Trust security model, ensuring that only compliant and trusted devices are granted appropriate network access. Unauthorized devices are restricted to protect the network.

Enforcement is achieved through ARP enforcement, which redirects and controls traffic from untrusted devices, applying Access Control Lists (ACLs) to manage permissions and restrictions. This process ensures that only authorized endpoints can communicate freely, while rogue devices are effectively isolated.

Finally, EasyNAC provides a robust alerting system, delivering notifications via multiple channels, including email, SMS, WhatsApp, Teams, Slack, and Syslog. This ensures that NAC administrators are promptly informed of any significant events, policy violations, or security threats, enabling swift and effective responses.

Overall, EasyNAC ensures a secure and compliant network environment through continuous monitoring, dynamic role adjustment, and comprehensive enforcement mechanisms. By integrating seamlessly with existing cybersecurity solutions and supporting various deployment scenarios, EasyNAC delivers a powerful and flexible solution for modern network security challenges.

End of Document