# EASY NAC

## TECHNICAL OVERVIEW



www.easynac.com

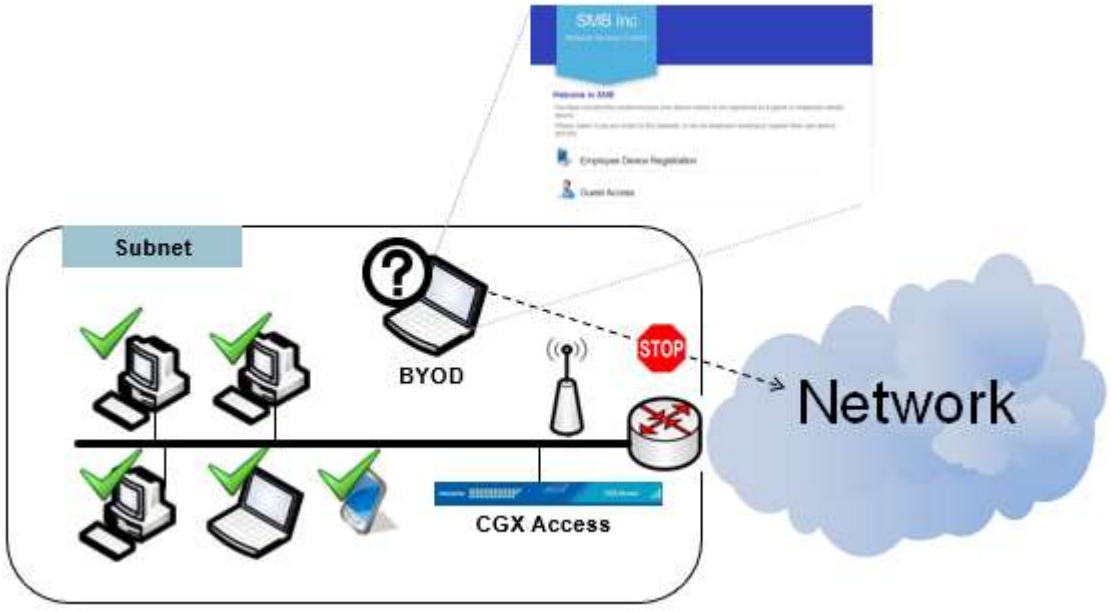
v3.0 201224

CONTENTS

# Overview

Easy NAC is an agentless network access control that provides strong security and is easy to deploy and manage. It implements a unique and innovative ARP enforcement method that provides robust network access control without the need for infrastructure changes. This means no VLANs to setup, no 802.1x implementations, no DHCP changes, no network changes at all.

The Easy NAC appliances are called CGX Access and can also be integrated with your existing cyber security solutions to provide additional compliance checks against managed endpoints. A single appliance can monitor and enforce up to 100 subnets. It works to manage ARP information on each subnet to effectively quarantine rogue endpoints. The process involves active and passive discovery of new/rogue endpoints, redirection using ARP management techniques, and filtering based on centrally managed ACLs.

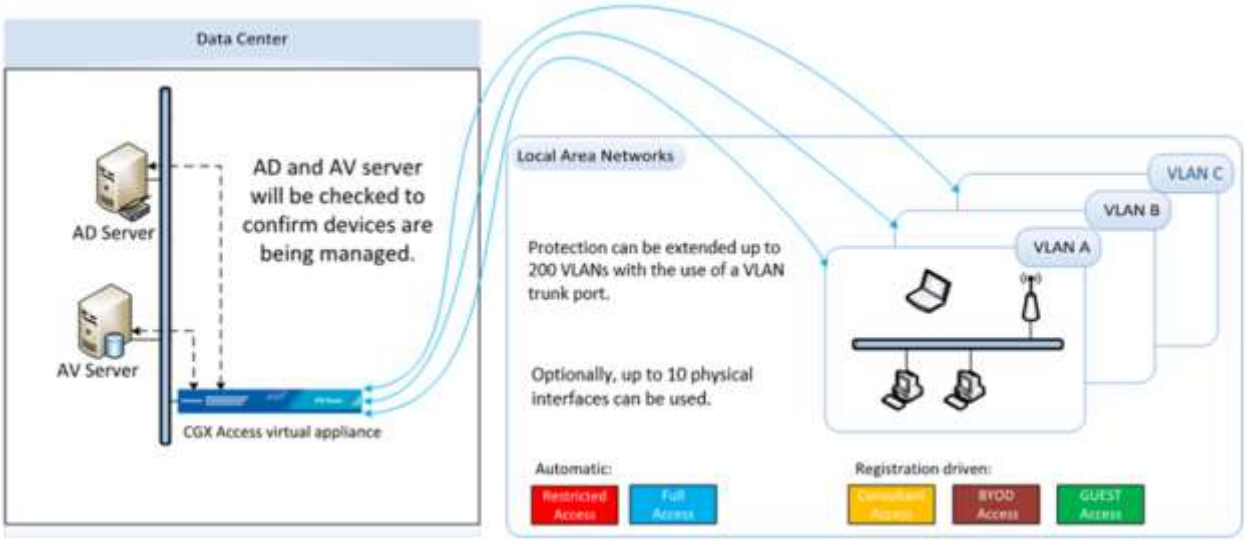



# Easy NAC Deployment Architecture

The CGX Access appliances are placed anywhere there is layer 2 connectivity for the subnets to be protected. There are three ways to connect a subnet to an appliance:

- **Method 1 – Physical connection**: Add additional network adapter and plug-in to a normal switch access port to extend protection to an additional subnet.

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



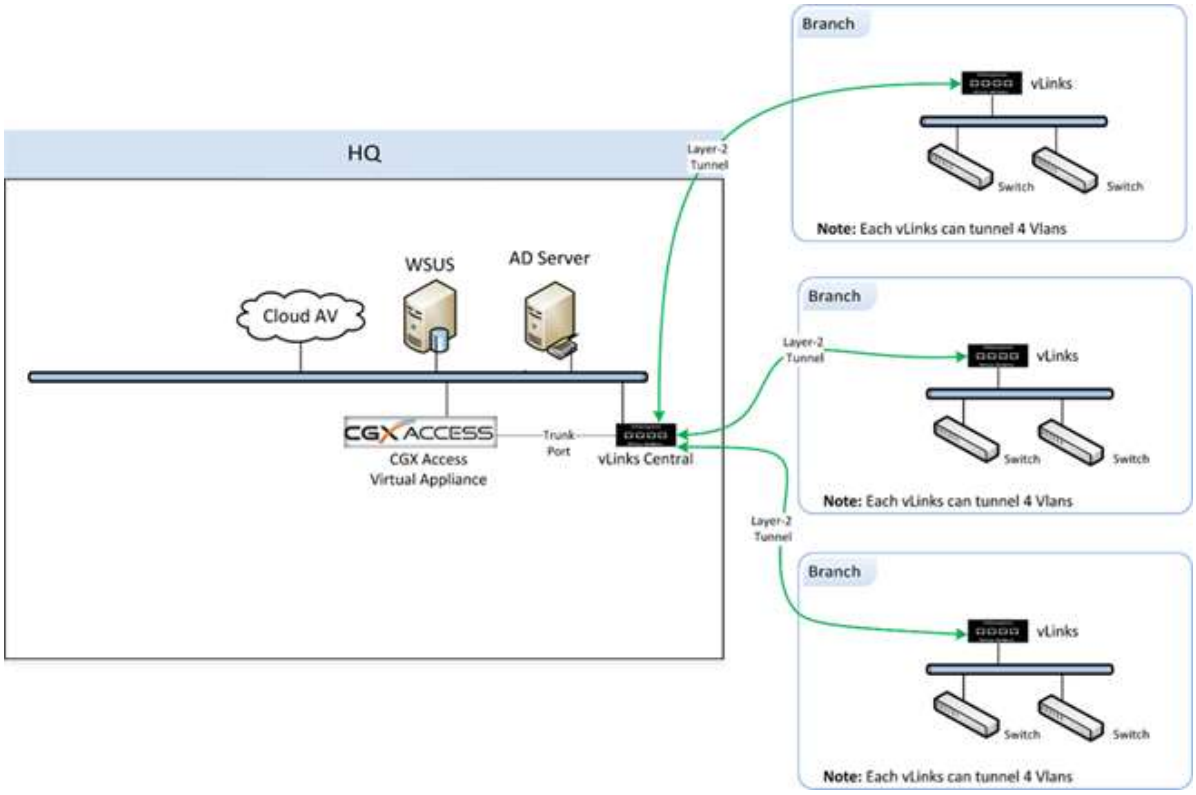

If there are remote locations and Layer-2 traffic can't be trunked back to the HQ appliance, then a separate CGX Access appliances can be deployed at each of the remote sites. A Central Visibility Manager can be used to managed these multiple appliances.

Note: for smaller remote sites where cost is a key concern, a vLinks appliance can be used to tunnel layer-2 traffic back to a centralized appliance using your existing layer-3 VPN or MPLS network.

- **Method 3 – vLinks**: For remote sites without either 802.1q or direct ethernet connections, place a vLinks at that site to extend layer-2 visibility back to the appliance.

  The CGX Access appliance requires layer-2 visibility of the subnets it's protecting. Having layer-2 visibility at the main site can be easily achieved with trunk ports or standard access ports. However, getting layer-2 visibility for remote sites can be more challenging. The vLinks solution is designed to extend the reach of the CGX Access appliances so it can also protect your smaller remote sites with cost effective hardware.

  The vLinks architecture is shown below. At remote sites, a vLinks appliance is placed on the network for layer-2 visibility. This layer-2 traffic is then tunneled back to a vLinks Central appliance. This tunneled traffic is sent over the existing corporate WAN, so an existing WAN network is required. MPLS and NAT'd network types are supported.




At the main site, a vLinks Central will consolidate the layer-2 traffic from multiple vLinks and share it with the CGX Access appliance using a port directly connected to the CGX Access appliance. With this connectivity in place, CGX Access will detect rogue devices at the branches and quarantine these devices real-time.  All Easy NAC features including compliance checks, captive portals, Automated Threat Response, etc., are supported.

# Device Discovery

Easy NAC use a combination of active and passive detection mechanisms to discover new endpoints when they join the network.

## DHCP DEVICES

When a new DHCP based endpoint connects to the network for example, it will send out a DHCP DISCOVER request. This broadcast packet will be seen by endpoints on the same subnet, including the CGX Access appliance. Once an IP address is assigned by your DHCP server, it will need to send out ARP requests on the network which is similar to the process described below in the static IP address devices.

## STATIC IP ADDRESS DEVICES

Statically addressed endpoints will send out layer-2 ARP requests, which are broadcast traffic, to locate endpoints and routers with whom they wish to communicate. CGX Access, being in the same broadcast domain, would be able to pick up the ARP request packets and immediately detect newly joined network devices. CGX Access will also periodically scan the network to detect systems that are stealthy connected to the network but without any DHCP nor ARP request.

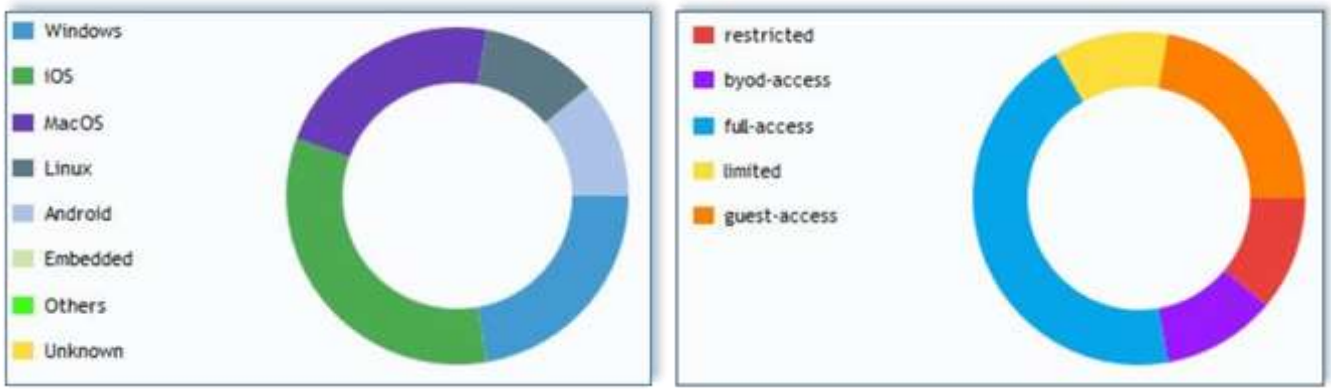
| MAC | IP Address | Hostname | Access Group | Roles | OS | Flags / Lists |
|---|---|---|---|---|---|---|
| 00:0C:29:4C:8C:B1 | 192.168.253.100 | WIN-EH9KPK2TKSH | full-access | full-access | Windows Server 2008 R2 Enterprise 7601 Service Pack 1 | network-infrastructure webserver virtual whitelist |
| 00:0C:29:4B:70:2E | 192.168.253.54 | MANAGED01 | restricted | untrusted | Windows 7 Professional 7601 Service Pack 1 | virtual |
| 00:0C:29:51:DB:AA | 192.168.253.50 | Sales-Mike | restricted | untrusted | Microsoft Windows XP | virtual |
| C0:25:E9:03:7E:B0 | 192.168.253.254 | | full-access | full-access | Linux 2.6.23 - 2.6.38 | network-infrastructure webserver |

# Device Profiling and Classification

## DEVICE PROFILING

Once CGX Access detects a new endpoint on the network, it will profile the device to determine which operation system (OS) it is running, and which network ports are open by using active and passive profiling techniques. Active Profiling includes network scanning such as NMAP and NBTScan which would detect an endpoint's OS, its open ports and grab the web server banner when it is detected on an endpoint.

Passive Profiling is accomplished by detecting the DHCP DISCOVER request broadcast packets and comparing them to the internal DHCP fingerprinting records to match up with the OS's unique identifier.




## DEVICE CLASSIFICATION

When CGX Access sees a new endpoint join the network, it determines the endpoint's role by checking its conditions against the Automated Device Classification Policy. Endpoints that have passed the device classification policy are considered authorized. They may be assigned full network access or partial network access depending on the role assigned.

**Automated Device Classification Policy**

Classify devices based on their characteristics

Activate | Cancel Changes

Add Rule

| Conditions | Actions taken when conditions are met | |
|---|---|---|
| Device is on routerlist | Set device role to full-access | |
| Device is on whitelist | Set device role to full-access | |
| Device is on blacklist | Set device role to restricted | |
| Has any of these flags: APT-Event, FP-mismatched, FW-Event, infected, IPS-Event, SIEM-Event | Set device role to restricted | |
| Has any of these flags: AV-off, AV-out-of-date, non-compliant, patch-failed, patch-pending | Set device role to non-compliant | |
| Has any of these flags: managed-device, full-access, AV-managed, AD-managed, network-infrastructure, router, switch, printer | Set device role to full-access | |
| Failed Agent Audit | Set device role to failed-agent-audit | |
| Passed Agent Audit | Set device role to full-access | |
| Completed Guest or Device Registration<br>Has any of these flags: byod | Set device role to BYOD | |
| Completed Guest or Device Registration<br>Has any of these flags: consultant | Set device role to consultant | |
| Completed Guest or Device Registration | Set device role to guest | |

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

Easy NAC provides Zero Trust security. If the endpoint cannot match any of rules in the device classification policy, it is considered an unauthorized device and will be assigned with an "untrusted" role. Easy NAC would quarantine the endpoint and hence its network access would be restricted.

# How a Device is Restricted

Easy NAC uses ARP Enforcement to provide network access control functionality without any network changes. ARP or Address Resolution Protocol is a basic and well understood TCP/IP standard. Easy NAC leverages ARP in such a way that it does not interfere with other authorized devices.

Once an unauthorized device is detected, the CGX Access appliance will automatically and regularly send out ARP REPLY packet to update the ARP table of the unauthorized device when it attempts to communicate. It will update the ARP table of any device the rogue is attempting to communicate with to ensure a trusted device doesn't communicate with the rogue device.

As a result of the ARP REPLY packets, traffic to and from the unknown device is now diverted to pass through the CGX Access appliance. This will have the immediate effect of restricting its network access of the untrusted device. An ACL can be configured, so the appliance will only forward packets that are permitted by the assigned ACL.

CGX Access use directed ARP REPLY and not ARP BROADCAST to enforce unauthorized endpoints. This means only unauthorized endpoints are redirected via ARP without introducing unnecessary traffic on the network. Authorized endpoints are permitted to use the network and it will not see any slowness or delay in terms of the network performance.

Unauthorized endpoints will not be able to bypass the above mechanism using Static ARP entries. CGX Access will still observe the attempted communication and the ARP updates will still be sent to the device that it attempts to communicate with.

For guest or BYOD access, the ACL can be configured to redirect any HTTP traffic to the Easy NAC captive portal for BYOD or Guest Access registration.

## ENFORCEMENT BY EXAMPLE

We have two hosts, Host A and Host B on a class C network. Initially, let's assume Easy NAC is not installed, to set a baseline. When Host A wants to communicate with Host B, it'll send out a broadcast ARP to try to find the destination MAC address for Host B's IP address. Host B will see the broadcast and reply to it, telling Host A how to get in touch. From there, communications can proceed between the two hosts.

Now let's add a CGX Access (CGXA) appliance. The first steps are still the same, Host A ARPs for Host B, and Host B replies. However, the CGXA, who saw Host A's ARP and knows it is an unauthorized endpoint, also replies to the ARP request, telling Host A that CGXA in fact Host B. This is done by CGXA replying to the ARP request giving its own MAC address as the match for Host B's IP address.

CGXA sends that reply several times to ensure that Host B's ARP update is immediately overwritten and will periodically re-send this reply to ensure that the redirection stays in place. This will cause Host A (the unauthorized endpoint) to communicate with the CGX Access appliance any time it wants to communicate with Host B, thereby preventing it from gaining network access.

There is also a slight variation to this scenario, and that is when Host B is on a different subnet than Host A. Again, Host A will ARP for Host B's MAC address, but since ARP is a layer two protocol, it will not extend beyond the current subnet, and will never reach Host B. However, the local router will recognize that this is an "off subnet" ARP request and it will automatically respond with its own MAC address. In effect, this tells Host A to send all off subnet traffic to the router, which can then forward it on to its final destination (Host B in this case).

If we now inject CGXA into the mix, the process stays the same, except the CGXA now redirects Host A and the router, instead of Host A and Host B. The ARP packets sent out by the CGXA are not broadcasts, and are updates only for the single host entry, so only quarantined endpoints will be affected by the ARP changes made on the router.

Based on the CGX Access "Restricted" ACL which would be applied to the unauthorized endpoint, it would be restricted to only allow DNS and DHCP request and redirection to the predefined captive portal for BYOD and Guest registration.

**End of Document**