ZERO TRUST - EASY NAC

HOW EASY NAC ADDRESSES ZERO TRUST REQUIREMENTS

www.easynac.com

v3.1.221223

CONTENTS

Overview

INTRODUCTION

Network Access Control (NAC) is a security solution that helps organizations enforce compliance and secure their networks by controlling access to network resources based on predefined security policies. It is an important component of a Zero Trust security model, which is a security paradigm that assumes that all network traffic is untrusted and requires strict verification before being allowed access to resources.

In the past, organizations have relied on a perimeter-based security model, which relied on firewalls and other security devices to protect the network from external threats. However, this approach has proven to be ineffective in today's increasingly mobile and remote workforce. With employees accessing the network from various locations and devices, it has become increasingly difficult to maintain a secure perimeter. Additionally, the rise of cloud computing and the use of third-party services has further complicated the issue, as organizations no longer control all aspects of their network.

The Zero Trust security model addresses these issues by assuming that all traffic is untrusted and requiring that all access be validated and authorized. NAC is an essential component of this model, as it provides the necessary controls to identify and authenticate users and devices before granting access to the network.

In this whitepaper, we will discuss how NAC, and Easy NAC specifically, can help organizations implement a Zero Trust security model and provide a high level of protection against cyber threats.

WHAT IS ZERO TRUST?

Zero Trust is a security model that assumes that all network traffic, whether it originates from inside or outside the organization, is untrusted and must be thoroughly verified before being granted access to resources. This approach is based on the premise that traditional perimeter-based security models, which rely on network segmentation and firewalls to separate trusted and untrusted traffic, are no longer sufficient to protect against modern cyber threats.

Instead, Zero Trust security models use a combination of technologies and processes to verify the identity and trustworthiness of users, devices, and applications before granting access to resources. This includes multi-factor authentication, contextual access controls, and continuous monitoring of user activity to detect and prevent security breaches.

HOW NAC HELPS IMPLEMENT ZERO TRUST

NAC is a security solution that helps organizations implement Zero Trust by controlling access to network resources based on predefined security policies. It works by requiring users and devices to authenticate themselves and meet certain security requirements before being granted access to the network.

For example, NAC can require users to authenticate using multi-factor authentication, such as a password and a security token, before being allowed to access the network. It can also enforce policies that require devices to meet certain security standards, such as having the latest security patches and antivirus software, before being granted access to the network.

In addition to controlling access to the network, NAC can also monitor user activity and alert security personnel to any suspicious activity. This allows organizations to detect and respond to potential security threats in real-time, helping to prevent security breaches and maintain a high level of protection.

WHAT IS EASY NAC?

Easy NAC is a third generation Network Access Control solution from InfoExpress Inc. that provides a comprehensive set of features to help organizations implement a Zero Trust Network Access (ZTNA) security mode.

Easy NAC was specifically designed to be simple and secure. It’s an agentless (agent optional) NAC solution that doesn’t require network changes, and is compatible with all types of switches (managed and unmanaged) , access points, wireless controllers, and all types of VPNs.   Easy NAC provides visibility and access control over all devices. It enhances security by preventing untrusted devices from joining the network, enforces baseline security, ensures least privilege access on BYOD and consultant devices, and monitors broadcast traffic for suspicious behavior. Easy NAC also integrates with Firewalls, APTs, SIEMs and other security appliances so it can quickly quarantine misbehaving or infected devices.

Key Features for Zero Trust

VISIBILITY AND CONTROL

Visibility is critical for zero trust as it enables organizations to have a clear understanding of the devices and users that are accessing their network, which is essential for enforcing access controls and ensuring compliance with security policies. With device visibility, organizations can gain a comprehensive view of their network and identify potential vulnerabilities, allowing them to take proactive measures to protect their assets and data.

Easy NAC provides both real-time visibly and real-time control. Easy NAC uses ARP enforcement so it has an IP address on every VLAN being protected. With its layer-2 visibility on every local subnet, Easy NAC can instantaneously detect any device connecting to the network, and block it immediately if is not trusted. Blocking is at the edge, so an untrusted device can't communicate with other devices, even if they are on the same VLAN.

Another benefit of ARP enforcement is that enforcement (control) can be enabled with no physical changes or configuration changes to the network. This is a key advantage of Easy NAC as it can work with any type of network infrastructure, and be quickly deployed.

COMPLIANCE CHECKING

Compliance checks are critical for a Zero Trust architecture because they help ensure that the organization's security policies and controls are being effectively implemented and enforced. Compliance checks help organizations to verify that their networks and systems meet industry standards and regulatory requirements. They also provide a way to measure the effectiveness of the organization's security controls and identify any gaps that need to be addressed.

Easy NAC provides both agentless and agent-based options for continuous compliance checking. If a device falls out of compliance, it can be restricted immediately.

Agentless compliance checks are performed by the Easy NAC appliance (CGX Access) integrating with leading Endpoint Protection Platforms and patch management solutions to verify the devices are being properly managed. A list of supported platforms can be seen here.

Agent-based compliance checks can work with all brands of EPP \ XDR platforms, and address more advance compliance & remediation requirements. Agents are supported on Windows 7+, MAC OSX and Linux platforms.

Often a hybrid approach can be used with agents being deployed on high-risk devices like laptops.

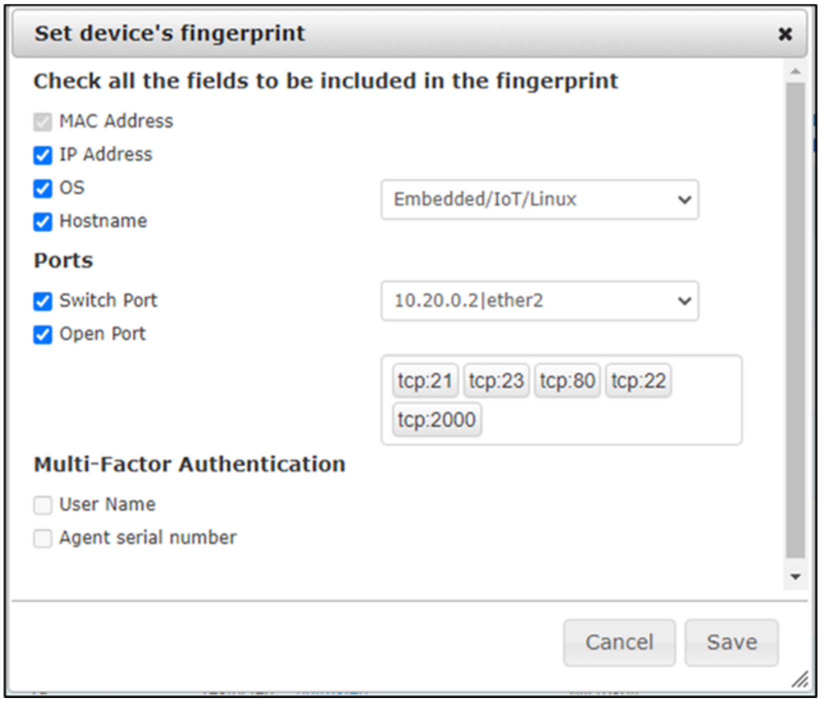
Below is a table summarizing Easy NAC’s agent-based vs agentless capabilities.

	Agents	Agentless
Detection speed	Continuous - Agent would detect changes in compliance status within a few seconds. (Real-time)	Continuous - Compliance checking interval depends on setup of the 3rd party solution we are integrated with. (Normally 5-10 minutes)
Supported OS	• Microsoft Windows 7+ • Apple MacOS • Linux	Depends on the OS supported by the 3rd party solutions we Integrate with
Compliance checks	Compliance check can be customized to Include but not limited to the followings: • Running Process • Registry values • Files and locations • Ini files and contents • Machine names and OS check • Authentication	Agentless solution – Integrations with AD, 3rd-party AV, Patch, and WMI A list of supported platforms can be seen here.
End-user compliance communication	Pop-up Message	HTTP and DNS Redirection
Real-time Wi-Fi adapters control	When connected to any wired network that has connectivity to CGX-Access (ie. Corporate Network). The wireless network adapter can be disabled automatically. It would be re-enabled once wired NIC is disconnected.	N/A Can use Windows Connection Manager as a substitute
Automatic Remediation	When a compliance check fails, a remediation action can be started. It includes running scripts or binary in the host that has the agent installed. With or without administrative rights.	N/A

DEVICE FINGERPRINTING

In a Zero Trust security model, all devices are untrusted until proven otherwise. This means that all access to resources must be validated, authenticated, and authorized before allowing access. NAC is an essential component of this model, as it provides the necessary controls to identify and authenticate users and devices before granting access to the network. However, many types of IOT and OT devices are not able to be authenticated and rely upon a technique called MAC Address Bypass that allows devices to bypass Network Access Control (NAC). This technique can also be used by attackers to gain access to a network and steal sensitive information or launch attacks against other systems

Easy NAC protects against this type of attack by providing a fingerprint feature to protect against MAC and IP address spoofing. All devices on the network are profiled for their MAC address, IP, Operating System, Hostname, open ports, and location. This information can then be used to set a specific fingerprint for each device. Once a fingerprint has been set, the device(s) will be protected from spoofing, as any variation on the fingerprint will trigger an alert and\or quarantine action.



Set device's fingerprint

Check all the fields to be included in the fingerprint

☑ MAC Address
☑ IP Address
☑ OS — Embedded/IoT/Linux
☑ Hostname

Ports

☑ Switch Port — 10.20.0.2|ether2
☑ Open Port — tcp:21 tcp:23 tcp:80 tcp:22 tcp:2000

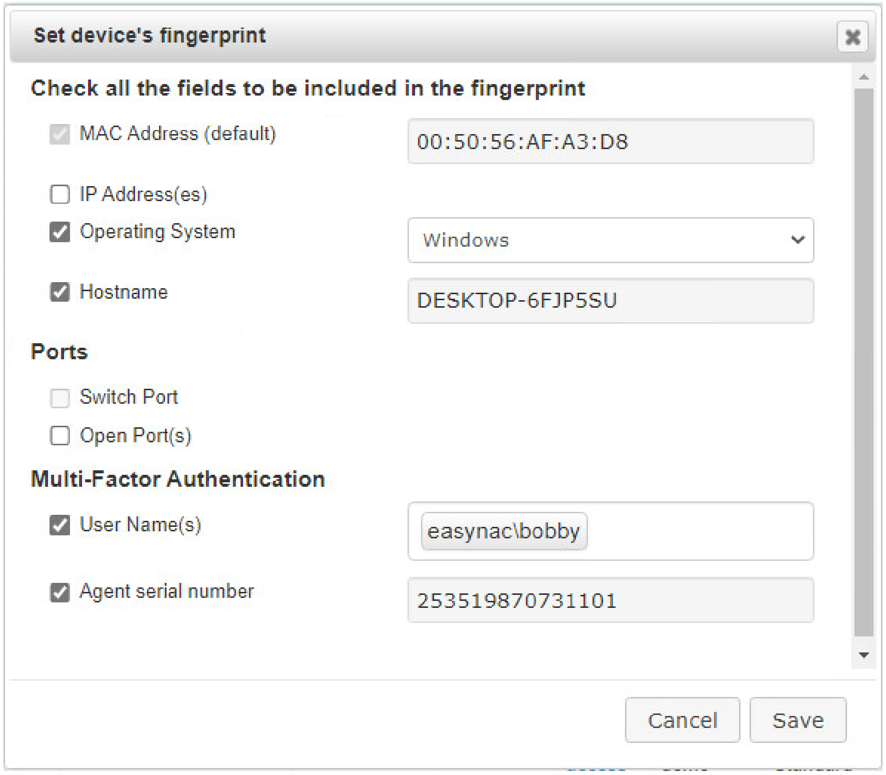
Multi-Factor Authentication

□ User Name
□ Agent serial number

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is important for Zero Trust because it provides an additional layer of security to verify the identity of users attempting to access a network. MFA ensures that even if a user's password is compromised, the attacker would still need a second form of authentication to gain access.

Levering its device fingerprinting capabilities, Easy NAC can provide an MFA solution that is transparent to the end-user. By monitoring the device's approved user ID and unique agent serial number. Easy NAC will verify a specific user is logged into a specific laptop with valid credentials.



Set device's fingerprint

Check all the fields to be included in the fingerprint

☑ MAC Address (default) 00:50:56:AF:A3:D8

☐ IP Address(es)

☑ Operating System Windows

☑ Hostname DESKTOP-6FJP5SU

Ports

☐ Switch Port

☐ Open Port(s)

Multi-Factor Authentication

☑ User Name(s) easynac\bobby

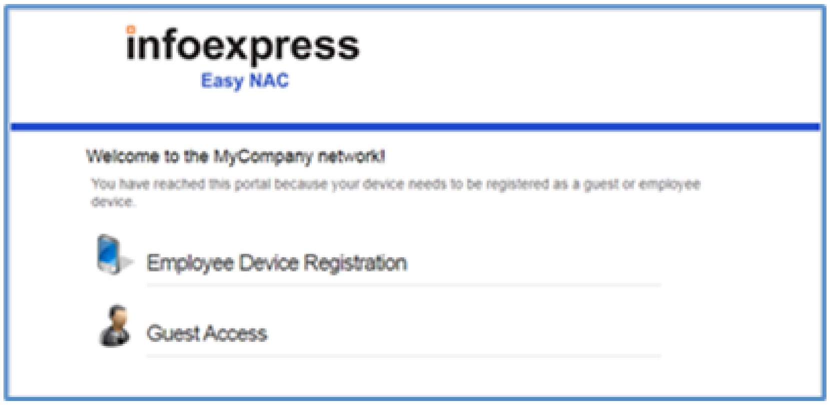
☑ Agent serial number 253519870731101

On the LAN and Wireless, this capability would be comparable to the use of digital certs for 802.1x authentication, but without the added costs or complexity of managing the digital certs deployment and renewal. The same Easy NAC MFA feature can also be leveraged to protect VPN access.

LEAST PRIVILIGE ACCESS

Zero Trust architecture generally requires least privilege access controls, which is a security principle that limits the access and privileges of users and applications to the minimum required to perform their intended function.

Easy NAC offers basic Role-Based Control features that are easy to implement for BYOD and consultant devices. A self-registration portal automates the BYOD registration and approval processes, and policies can be set by groups, user or device to limit network access.



infoexpress
Easy NAC

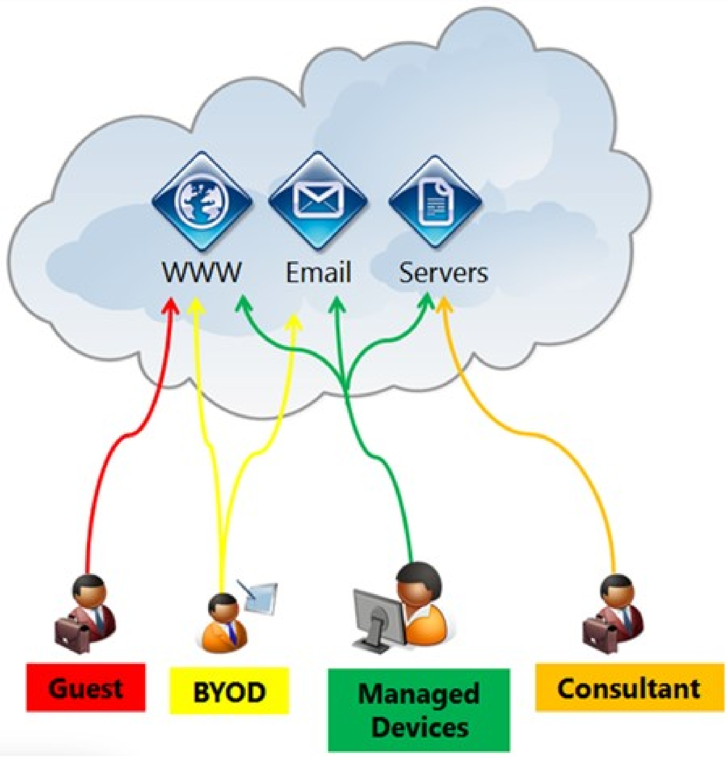
Welcome to the MyCompany network!

You have reached this portal because your device needs to be registered as a guest or employee device.

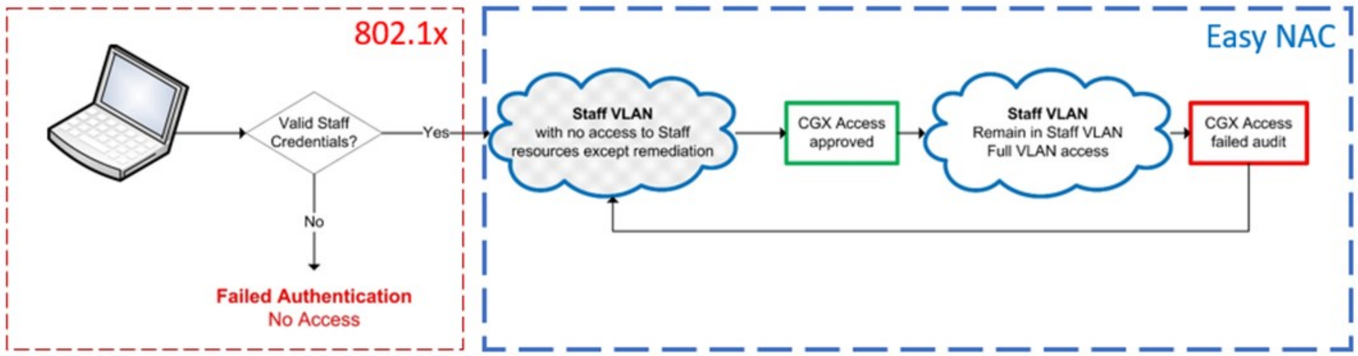
Employee Device Registration

Guest Access

By Leveraging ARP enforcement, ACLs are then applied to limit guests to internet only access. While consultant devices can be limited to specific resources, they need to complete their work.



For more advance capabilities, there are multiple third-party solutions available to implement least privilege access ranging from dynamic Group Policy Objects, VLAN assignments, Cloud Security Gateways and more. Easy NAC is network agnostic and can co-exist with any of these approaches. For example, a customer could configure its switches for 802.1x authentication and then assign VLANs based on authentication.



With this approach, the switches with 802.1x would assist with least privilege access control, while Easy NAC would provide traditional NAC features like compliance checks, device fingerprinting, MFA, BYOD access control, etc. 802.1x with Easy NAC has many deployment and security benefits over traditional RADIUS NAC.

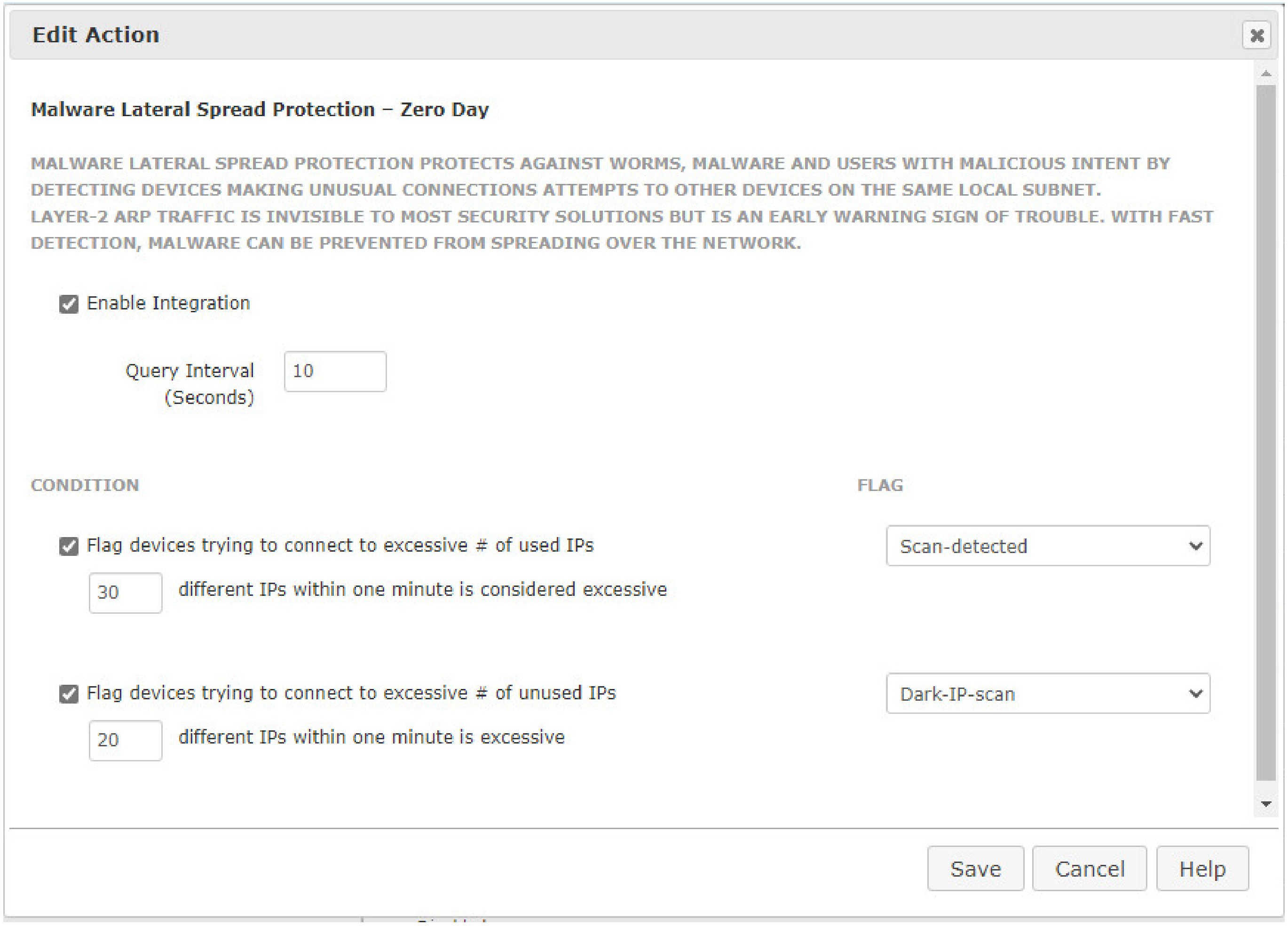
In the future, If the customer decides to disable 802.1.x and leverage a Cloud Security Gateway solution, Easy NAC would still provide Zero Trust benefits.

MONITORING

Monitoring network traffic is important for implementing a zero-trust security model because it allows organizations to identify and mitigate potential threats, such as malware or unauthorized access attempts, in real-time.

With its layer-2 visibility, Easy NAC is in a unique position to detect devices making unusual connection attempts to other devices within the same segment. If an end-user device suddenly attempts to connect to an excessive number of devices on the same subnet, or trying to connect to Dark IPs, IP’s not active on the network, this is very suspicious behavior. This behavior is indicative of a network scan being performed or malware trying to probe the network in an attempt to spread.

Easy NAC can detect this behavior and immediately quarantine this device so it can’t spread malware laterally on the network.



Edit Action

Malware Lateral Spread Protection – Zero Day

MALWARE LATERAL SPREAD PROTECTION PROTECTS AGAINST WORMS, MALWARE AND USERS WITH MALICIOUS INTENT BY DETECTING DEVICES MAKING UNUSUAL CONNECTIONS ATTEMPTS TO OTHER DEVICES ON THE SAME LOCAL SUBNET.
LAYER-2 ARP TRAFFIC IS INVISIBLE TO MOST SECURITY SOLUTIONS BUT IS AN EARLY WARNING SIGN OF TROUBLE. WITH FAST DETECTION, MALWARE CAN BE PREVENTED FROM SPREADING OVER THE NETWORK.

☑ Enable Integration

Query Interval (Seconds): 10

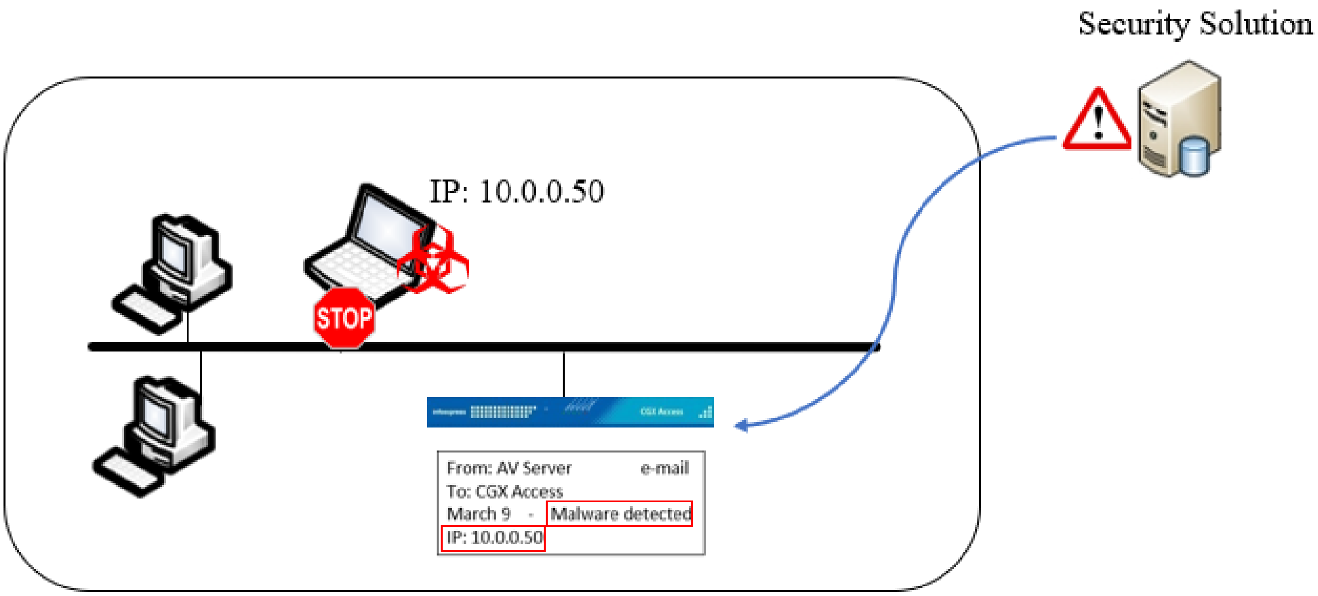
CONDITION	FLAG
☑ Flag devices trying to connect to excessive # of used IPs 30 different IPs within one minute is considered excessive	Scan-detected
☑ Flag devices trying to connect to excessive # of unused IPs 20 different IPs within one minute is excessive	Dark-IP-scan

ORCHESTRATION

A comprehensive Zero Trust strategy typically involves implementing multiple solutions and technologies. Therefore, orchestration plays a crucial role in Zero Trust by providing a unified and centralized way to manage and enforce security policies.

Orchestration allows for the automation and coordination of security controls across different security solutions, such as endpoint protection platforms, firewalls, SIEMs, intrusion detection and prevention systems, and identity management systems, so that they can work together to provide a faster mitigation of security incidents.

Easy NAC was designed to work with a wide range of security solutions. Easy NAC can receive event-based syslog messages or e-mail alerts from all types for security devices and take immediate action to quarantine the device.   Any device that can send an alert can integrate with Easy NAC.

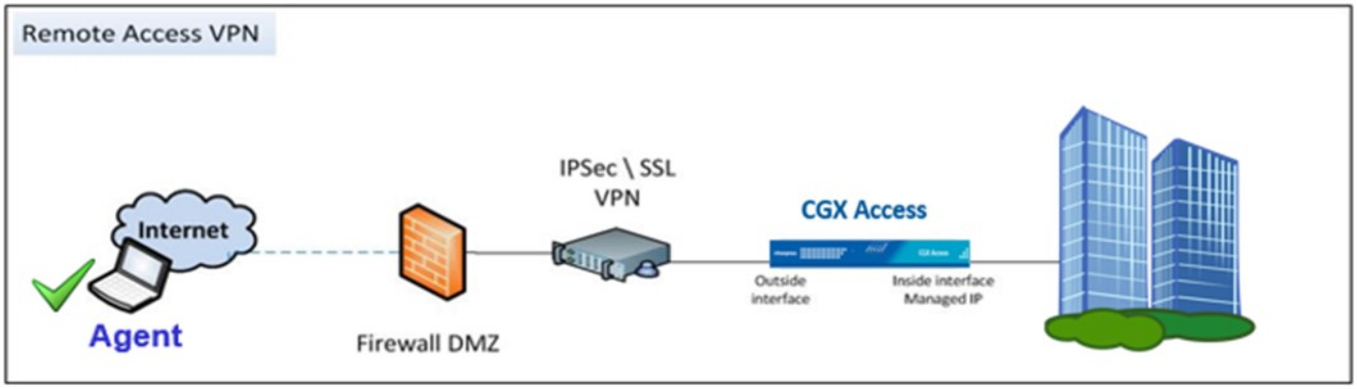


Easy NAC's ability to quickly quarantine a device based on 3rd party alerts will dramatically reduce the Mean Time to Response (MTTR) to security incidents.

VPN PROTECTION

Without proper protection, a VPN could be vulnerable to various cyber threats such as hacking, compromised credentials, and malware, which could compromise the security of the entire network. In a Zero Trust architecture, all resources and access attempts are verified and authenticated, ensuring that only authorized users and devices have access to sensitive information. This added security measure helps to protect the VPN and the organization's resources from unauthorized access and potential breaches.

As an overlay solution, Easy NAC can work with any VPN to provide the Zero Trust Principles. The Easy NAC appliance (CGX Access) is deployed in line behind the existing VPN. Devices would need to be compliant with security policies in order to gain access to the corporate network.



The Fingerprinting with Multi-Factor Authentication feature can also be enabled to confirm the remote user has a correct corporate issued device. This would protect against credential theft without requiring the user to have a have a security token.

The inline appliance could also enforce Least Privilege Access polices in line with ZTNA principles.

Conclusion

Network Access Control is an important component of a Zero Trust security model, as it helps organizations enforce compliance and secure their networks by controlling access to network resources based on predefined security policies. By requiring users and devices to authenticate themselves and meet certain security requirements before being granted access to the network.

Without needing to rearchitect the network, Easy NAC provides a comprehensive set of features that helps organizations implement a ZTNA security model, including full visibility and control, continuous compliance checks, device fingerprinting, multi-factor authentication, least-privilege access, monitoring, orchestration and reporting. These flexible features work together to increase visibility, improve security, and simplify security management, which can help organizations protect their networks from unauthorized access and reduce the risk of a security breach.

End of Document