



How to Get NAC Up-and-Running in One Hour

For Check Point Firewall or Endpoint Security Administrators

Contents

Introduction	3
Defining an Organization’s Requirements for NAC	3
Two Paths to NAC—Port vs. Gateway	4
Deciding if Port or Gateway NAC Is Right for an Organization	4
Issues for Deploying Port-based NAC	5
Deploying Gateway-based NAC	5
Using the Check Point Security Gateway for Gateway-based NAC	6
Configuration	6
Conclusion	9

Introduction

The ability for enterprises to control access to their networks is vital for security and compliance. Network access control (NAC) ensures that only policy-compliant individuals and machines can access resources on a network. NAC also blocks malware, prevents data breaches, and helps with regulatory compliance.

The idea of NAC is to control access through network-based enforcement, such as on a switch or gateway. Access control policies are based on a user's identity and business authorizations. With NAC, access control is centralized, granular, auditable, and strong.

The promise of NAC is huge, but so are the evolving (and competing) architectures that are typically complex, difficult and expensive to deploy and manage. Consequently, after years of promise, many organizations have yet to tap the benefits of NAC.

Check Point offers a quick way to deploy NAC and get its benefits – without getting bogged down in complex deployment scenarios. With a Check Point firewall, organizations can get policy-based NAC up-and-running in an hour. This white paper describes how.

Defining an Organization's Requirements for NAC

The process of choosing a NAC solution involves a number of decisions. An organization must assess its degree of risk related to unauthorized access, determine which NAC technology will mitigate the risk, establish how quickly a solution is required, and evaluate the cost and effort associated with that solution.

Here is what an organization should expect from a NAC solution:

- NAC will enforce policy for different sets of users depending on how and where they enter the network. The NAC enforcement mechanism will ensure that security policy is automatically applied to all endpoints using the network – including remote workers, network guests, mobile workers and partners.
- Typical policies for NAC will relate to use of up-to-date antivirus and antispyware software, disk encryption status, approved endpoint firewall rules, software patches, specific versions of authorized applications, and correct registry entries.
- NAC may be applied to managed assets (employee PCs, devices) and unmanaged assets (devices owned by guests, some printers).
- NAC will quarantine unsafe endpoints and automatically bring them into compliance. Productivity will be ensured by sandboxing a user to permit working while the endpoint is fixed.
- NAC will restrict network access by unknown guests.

NAC Glossary

Network Access Control (NAC) – Security protocols for controlling access to a network based on policies and user identities. Similar to NAC frameworks with other acronyms (see related sidebar).

Pre-admission vs. Post-admission – Enforcement of NAC policy either before or after a user or machine accesses the network. Pre-admission might consist of requiring an endpoint to update antivirus signatures before access. Post-admission usually monitors endpoint compliance after a user has accessed the network.

Remediation, Quarantine and Captive Portals – NAC technologies that automatically repair endpoints (e.g. update antivirus signatures) before granting access. Quarantine is a restricted IP network that allows employees to continue working while an endpoint undergoes remediation. A captive portal can help automate repair via the web.

Cooperative Enforcement – NAC technology from Check Point that uses a firewall, VPN server, switch, or wireless access point as an enforcement point to quarantine and remediate hosts that fall out of compliance with a gateway security policy.

EAP – The Extensible Authentication Protocol is a universal framework for authenticating users in wireless networks and point-to-point connections. EAP is used to define message formats.

802.1X – An IEEE standard for port-based authentication. Authentication requires communications between a supplicant (client software), authenticator (switch or wireless access point), and authentication server (usually a RADIUS database).

Two Paths to NAC—Port vs. Gateway

With NAC, access control is typically performed by the network infrastructure. There are two fundamental paths for deployment of network-enforced NAC. The first taps the traffic control capabilities of ports on an 802.1X-compliant network switch. Port-based NAC is supported by several NAC frameworks (see sidebar). The other path is gateway-based, which applies access controls between networks. Other non-network infrastructure enforcement methods exist such as DHCP, IPSec, and self-enforcement; however, these methods are not covered in this paper.

Port-based NAC uses 802.1X to enforce strict switch port security. All hosts authenticate using an Extensible Authentication Protocol (EAP) supplicant before being granted layer 2 data-link access (e.g. Ethernet) to a network. A port-based solution will quarantine non-compliant devices at the network edge.

A gateway-based NAC solution is different; it performs restriction at the layer 3 network level (e.g. IP). An EAP supplicant is not required although an agent is used to perform identification of the endpoint and to perform health policy checks. A gateway-based solution will quarantine between networks.

The following table compares features of port- and gateway-based NAC:

NAC Features	Port-based	Gateway-based
Enforcement type	802.1X	Cooperative Enforcement
Enforcement point	Switch, wireless access point	Firewall
OSI enforcement layer	Layer 2 (Data-link)	Layer 3 (Network)
Quarantine scope	VLAN or port ACL	Gateway, network edge

Table 1. Comparing features of port- and gateway-based NAC

If the primary goal of an organization’s NAC project is to prevent unauthorized machines from plugging in to a network, an 802.1X-based solution may be the best path. However, if the organization’s goals are more to perform endpoint health checks and ensure policy compliance, a gateway-based NAC is a simpler and more cost effective solution.

Deciding if Port or Gateway NAC Is Right for an Organization

The complexity of NAC frameworks has earned it a reputation for being hard to deploy and manage. It’s easy to find roadblocks, which is why aspirations for NAC have stalled in so many organizations. But many users need NAC now because their security posture is weak, and threats are growing every day. As a result, organizations are implementing NAC in ways that are different from its debut in 2003-04¹. For some, port-based NAC is still a requirement. Gateway NAC, however, allows administrators to get the most important benefits of NAC right away, without the complexity and costs of using switches for enforcement.

NAC Frameworks

Several NAC frameworks provide systematic, policy-based means for controlling network access via ports on a switch. The frameworks were originally based on 802.1X, but have expanded to unify other endpoint security technology. Implementing a NAC framework is complex and can require significant change to an organization’s network infrastructure. The frameworks include:

TNC – Trusted Computing Group’s Trusted Network Connect. Framework by a multi-vendor consortium that aims to provide endpoint integrity at every network connection in a multi-vendor network.

NEA – IETF’s Network Endpoint Assessment. NEA is a standards-driven development of open protocols for access control based on policies governed by an endpoint’s security posture. It’s designed for multi-vendor interoperability and is correspondingly complex.

CNAC – Cisco Network Admission Control. Framework by Cisco Systems, Inc. that restricts access based on identity or security posture. A key component is the Cisco Trust Agent that allows endpoints to communicate with Cisco routers.

MSNAP – Microsoft Network Access Protection. Framework by Microsoft Corporation to control access of a computer based on system health of that host. Administrators configure policies to govern compliance for access. MSNAP is typically deployed in Microsoft-centric networks.

¹ Gartner, “Magic Quadrant for Network Access Control” (27 March 2009)

Issues for Deploying Port-based NAC

Deploying port-based NAC is a complex process. Many skills are needed to configure 802.1X products in large deployments. The network security team needs to know how to upgrade and configure the organization's switches to support 802.1X, segment the network using VLANs, configure RADIUS servers, interface with various user directories, and configure and roll-out EAP supplicants. When planning an 802.1X infrastructure, organizations should consider what NAC standards (if any) will be required to achieve the NAC deployment's end goals. Typically, the goals will dictate what specific RADIUS servers, supplicants, and other additional components may be required for a successful deployment.

It's also important to understand the inherent limitations in port-based NAC. A typical enterprise will want to attach many devices to the network that don't support 802.1X, such as older printers and phones. A strategy will be required to prevent people from using the physical ports of these devices to obtain unauthorized access. The organization will also want to have some idea of how to grant access to guest workers who won't necessarily be able to participate in its 802.1X architecture. These aren't easy problems to solve, and they often times involve upgrading equipment or buying new NAC architecture components such as captive portals, endpoint profiling servers, and other ad-hoc stop gaps.

Despite these challenges, Check Point is not against port-based NAC. Check Point has a long history of supporting and integrating with numerous NAC technologies, beginning with VPN device integration (Cisco, Nortel, Check Point) and later 802.1X. We sell port-based NAC to meet customer requirements. If those requirements mandate the functionality of 802.1X, organizations should be prepared to implement a solution with a multitude of "moving parts"—and their associated technological complexity.

Deploying Gateway-based NAC

It became apparent early on that 802.1X could only be deployed in certain networks under very controlled circumstances. What users needed was a way to leapfrog the complexity of 802.1X without losing the most important benefits. The result is gateway-based NAC. Rather than enforcing policy at the port level like 802.1X, the firewall integration enforces policy at the network segment/gateway level. For example, a common objective for NAC is to ensure that a user's device is in compliance with the organization's endpoint policy. Such a policy could potentially require the presence of anti-virus software or a specific Microsoft Service Pack on all endpoints. With gateway NAC, if a non-compliant device attempts to connect to the network, the gateway firewall will restrict the host and redirect its web traffic to a captive portal. Turning on the firewall NAC feature in a network with this integration can be done in an hour; by comparison, 802.1X implementations can take months. This firewall NAC integration provides many of the same benefits as port-based NAC without the associated costs.

Using the Check Point Security Gateway for Gateway-based NAC

The Check Point gateway NAC solution requires a R65 (and above) Security Gateway and Endpoint Security R70 (and above). There are no new licenses required beyond these two products. The rest of this section describes the steps necessary to enable gateway-based NAC.

Endpoint Security uses the firewall as an enforcement point to quarantine and remediate hosts that fall out of compliance with a gateway policy. This NAC capability is called “Cooperative Enforcement.” Using Cooperative Enforcement, a gateway policy can require connecting clients to possess a minimum set of virus definitions or prohibit the use of a specific application (e.g., Skype or AIM). Clients that fall out compliance with the gateway policy can be disconnected, restricted, or placed into network quarantine. For example, a Check Point Security Gateway can restrict network traffic for clients that have fallen out of compliance with the enterprise security policy. When a policy violation occurs, a popup message is displayed from the Endpoint Security client’s tray icon. After a period of warning, the gateway firewall will restrict the host and redirect all client web traffic to a captive portal like the one shown in the screen shot below.



Cooperative Enforcement Captive Portal

Once the user has taken manual action to correct the problem or auto-remediation completes, the restriction is lifted and the client is removed from the firewall quarantine.

Alternatively, an administrator can choose to enforce an alternative set of gateway firewall rules rather than capturing traffic to a quarantine portal when an endpoint is out of compliance. In the case of hosts that do not or are not capable of running an endpoint agent (printer, phone, etc.), these devices can be exempted from the cooperative enforcement policy. Typically, however, these devices do not have an operational need to pass traffic through a gateway enforcement point.

Configuration

Configuration is a simple three-step procedure. First, Cooperative Enforcement must be enabled on the Check Point Security Gateway. Second, the Endpoint Security server must be configured to perform Cooperative Enforcement with the Security Gateway. Third, enforcement rules must be created and added to a policy.

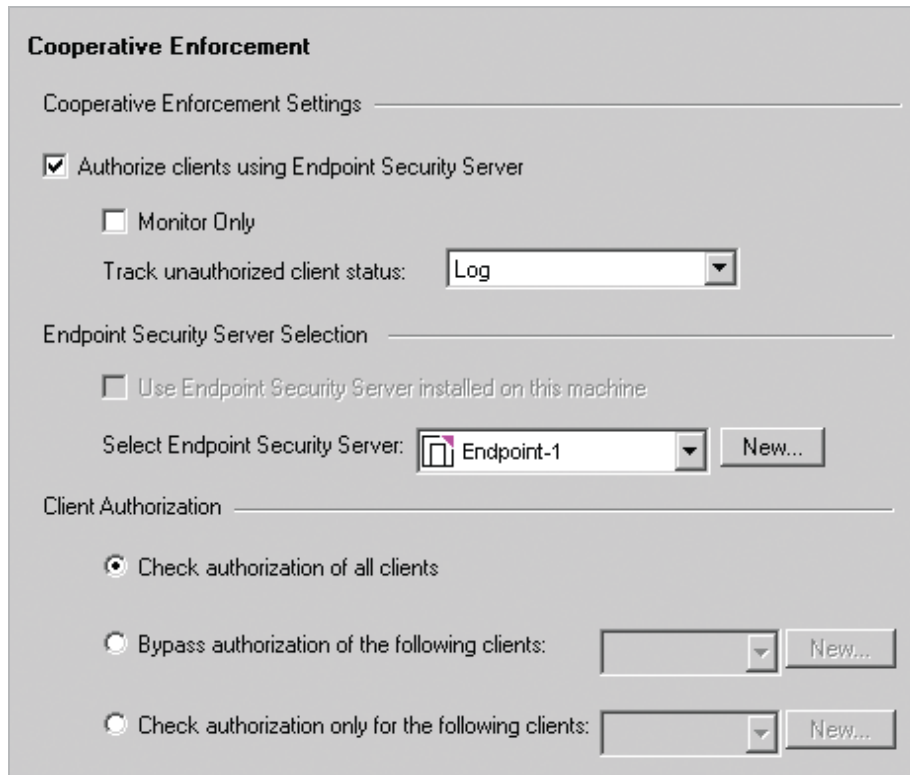
Check Point Endpoint Security

Check Point Endpoint Security™ is the first and only single agent that combines all essential components for total security on the endpoint:

- Highest-rated firewall
- Antivirus, anti-spyware
- Full-disk encryption
- Media encryption with port protection
- Network access control (NAC)
- Program control and VPN

Check Point Endpoint Security protects PCs and eliminates the need to deploy and manage multiple agents, reducing total cost of ownership.

The administrator will start by launching the SmartDashboard application and connecting to the SmartCenter. Double-click the firewall gateway from the Network Objects list. Next, navigate to the Cooperative Enforcement configuration screen. Choose the “Authorize clients using Endpoint Security Server” check box and select the organization’s Endpoint Security server from the drop down box as seen below.

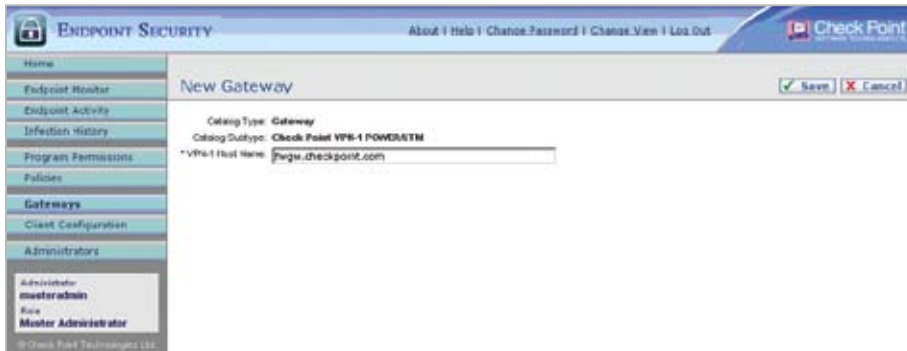


Click the “OK” button to return to the dashboard. Finally, select “Install Policy” from the Policy drop-down.

On the Endpoint Security server, navigate to the Gateway Manager and define a new “Check Point VPN-1 POWER/UTM” gateway as seen below.



On the New Gateway screen, enter the host name or IP address of the Security Gateway that will be enforcing the Cooperative Enforcement gateway NAC policy. Click “Save” when complete.



Finally, define an enforcement rule. Within a policy, click on the “Enforcement Settings” tab and choose the “Add” button. Choose “New Rule” followed by “Enforcement Rule.” (Alternatively, an Anti-virus or Client rule can be used.) For testing purposes, create a simple rule that looks for the presence of a file or registry entry on an endpoint as pictured below.

* Rule name:

Operating systems:

Rule Conditions

Specify the conditions this rule will check for.

Check for registry key and value

 * Registry Key:

 Value:

Check for file and properties

 * File Name:

File Properties:

Running at all times

Location (full path excluding filename):

Version number: Min.: Max.:

Last modified less than 'n' days ago:

Match Smart Checksum:

Click “Save” when complete. Select the newly created enforcement rule and click “Add.” To save your policy, click the “Save” button.” That’s it! Congratulations – this simple process allowed the setup of gateway NAC in under an hour.

Conclusion

NAC can provide an organization with powerful, granular control of endpoint network access. Port-based NAC deployment is challenging, but gateway NAC can deploy in one hour with a Check Point firewall. Check Point Endpoint Security includes support for both port-based and gateway-based solutions. The policy-based controls provided by gateway NAC will be sufficient for many organizations. Doing a pilot project with gateway-based NAC is a simple process that allows an organization to leverage an existing Check Point firewall. The firewall will be the gateway enforcement point for policy-based NAC. We invite your organization to contact its Check Point sales representative to learn more about NAC capabilities it may already own, and how these can be leveraged with the NAC functions of Check Point Endpoint Security.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.