Understanding Network Access Control
Technology Concepts and Solution Planning Guide
# Table of Contents

Introduction ............................................................................................................. 3  
Understanding NAC .............................................................................................. 3  
Preparing for NAC ................................................................................................. 4  
  The Overall Goal .................................................................................................. 4  
  End Systems and Users to be Supported ............................................................. 5  
Implementation ....................................................................................................... 6  
Detect & Authenticate ............................................................................................ 6  
  802.1X ................................................................................................................. 7  
  MAC Based Authentication (via RADIUS) ........................................................... 7  
  Web Based Authentication .................................................................................... 8  
  Static Port/MAC Configuration .......................................................................... 8  
  Dynamic Port/MAC Configuration (SNMP) ......................................................... 9  
  Kerberos Snooping .............................................................................................. 9  
Assessment .............................................................................................................. 10  
  Agent-less ........................................................................................................... 11  
  Agent-based ....................................................................................................... 12  
Authorization .......................................................................................................... 13  
  (Port) VLAN Allocation ..................................................................................... 13  
  Policies .............................................................................................................. 14  
  Disabling Ports ................................................................................................... 15  
Remediation ............................................................................................................ 16  
Monitoring ............................................................................................................. 16  
Beyond Network Security ....................................................................................... 17  
  NAC and VoIP .................................................................................................... 17  
  NAC and the Security Infrastructure .................................................................. 17  
  NAC and Virtual Servers .................................................................................. 17  
  NAC and the IT Helpdesk ................................................................................ 17  
Summary .................................................................................................................. 17  
Appendix .................................................................................................................. 18  
  Attachment A: Example Checklist Roles/Rights ................................................. 18  
  Attachment B: Example Checklist Infrastructure ............................................... 18  
  Attachment C: Example Checklist Assessment Checks ................................. 18  
  Attachment D: Example Checklist Reporting .................................................. 18
Understanding Network Access Control

Introduction

Network Access Control (NAC) solutions deliver a comprehensive approach to identifying, controlling, and securing access to critical network communications and business services. Well architected NAC solutions proactively manage whether a trusted user, a guest, or a device can connect to a network and what they are authorized to do once connected; this is all based on policy criteria such as device and user identity, business role, time of day, location, and health of the end system. Comprehensive NAC solutions use both agent-based and agent-less assessment technologies, along with proactive and reactive policy enforcement to provide a solid pre-connect and post-connect end system security offering.

A well architected NAC solution will leverage a number of important functions including end system detection, authentication, assessment, authorization, and remediation. This more easily enables IT organizations to quickly deploy NAC, and more importantly, to enable phased deployment to best align with business needs.

Throughout this paper, a graphical representation of several key business variables will be offered as guidance related to specific NAC technologies. A template is detailed below for reference.

Understanding NAC

NAC is an acronym which stands for Network Access Control. Sometimes it is also referred to as Network Admission Control. NAC is a common term within IT organizations today, but there is much discussion around what NAC involves and what it does not. Some view NAC as simple registration and authorization of network connected end systems. Some view NAC as a solution to protect the network environment from viruses and worms. Some view NAC as a gatekeeper function to control how end systems and guest systems, which are not compliant with corporate computing guidelines, can access the network. A well architected NAC solution is actually all of these things. Network Access Control is the integration of several technologies to provide a solution that proactively and reactively controls end system communication on the network. There are a number of individual functions that make up a comprehensive NAC solution.
• **Detect** - Detection and identification of new devices connecting to the network
• **Authenticate** - Authentication of users and/or devices
• **Assess** - Assessment of end systems regarding their compliance and/or vulnerabilities
• **Authorize** - Authorization to use the network based on the results of the authentication and the assessment
• **Monitor** - Monitoring users and devices once they are connected to the network
• **Contain** - Quarantine problem end systems and/or users to prevent them from negatively impacting the overall network environment
• **Remediate** - Remediation of problems with the end system and/or user

A well architected solution should integrate highly advanced, policy-enabled network infrastructure, along with advanced security applications and centralized management to deliver all of the required functions for pre and post-connect secure network access.

### Preparing for NAC

NAC, if deploying corporate-wide, can be an extensive project and will require thorough preparation. The following information will describe some of the preparation that an IT organization can perform to ensure a successful NAC deployment.

### The Overall Goal

Before embarking on a project to implement NAC, it is important to understand the major business benefits you plan to accomplish with the NAC solution. An example might be as follows:

“We would like to implement NAC to ensure our guests can access the internet in our conference rooms. Guests should not be allowed to communicate or connect to our internal systems. All end systems connecting to our network should have a minimum level of security.”

With this example, fundamental elements for a NAC project could be determined:

• **Who** is allowed to connect to the network?
• **How** are they allowed to communicate?
• **What** are they allowed to connect to?
• **Where** should they get access?
NAC generally is a process and can be separated into:

- **Roles** (who?)
- **Rights** (how?)
- **Resources** (what?)
- **Location** (where?)

A time component can also be added (when can one access?).

It is important to define all this information before embarking on a NAC deployment. A possible representation for the above example could be:

<table>
<thead>
<tr>
<th>Role</th>
<th>Rights</th>
<th>Resources</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Employee</td>
<td>Applications</td>
<td>Application server</td>
<td>Office</td>
</tr>
<tr>
<td>Guest</td>
<td>Only HTTP</td>
<td>Internet gateway</td>
<td>Conference rooms</td>
</tr>
</tbody>
</table>

Often a description of roles and rights already exists within a local directory or within the corporate structure itself. It often makes sense to use those rules (or groups) as a base for the NAC concept. A local directory can only be used as a starting point since most of the network systems are generally not users. In a typical enterprise network, only 30-50% of all end systems are desktops or laptops. The greater percentage consists of a diverse array of devices with different rights.

**End Systems and Users to be Supported**

One of the challenges of a NAC implementation is the integration of different types of end systems. Considering the diverse options of identification, authentication, and assessment at the connection point to the network, it can be difficult to ensure complete network coverage with a NAC solution. To ensure a comprehensive deployment of NAC, it will be important to understand in advance what types of end systems exist and what rights they should have in the network environment. Groups and resources need to be assigned for end systems as well as the end users. The groups should not be too specific as the administrative effort should remain at a minimum.
Some Preparation Questions:

- Are all types of network users and devices known?
- Have all required resources for the defined groups been identified?
- Are there any physical or logical restrictions? Should there be temporal restrictions?
- Can resources be grouped together?
- Should access be granted generally and denied specifically or vice versa?

Even if you only start out with some of the device or user groups, you need to have a full view of all of them in order to choose the right NAC architecture. An agent-based solution for NAC for example, would not be applicable for all end systems and devices like printers, VoIP phones, and others. This could cause problems after the roll out as many of your own clients will not be manageable.

Implementation

A phased approach for implementing a NAC solution is the preferred method. In general, a NAC implementation can be separated into the following phases:

- **Phase 1: End-System Detection and Tracking**
- **Phase 2: End-System Authorization**
- **Phase 3: End-System Authorization with Assessment**
- **Phase 4: End-System Authorization with Assessment and Remediation**

**Phase 1:** Collects information about all end systems without altering any existing network access. This is basically an inventory of end systems attached to the network. This can be done with or without authentication.

**Phase 2:** Considers pre-defined rules and restrictions related to network access. This typically requires authentication to ensure unique network access policies can be enforced for each end system and user.

**Phase 3:** Assessment of all end systems. This data can be accessed via an external management system (for software distribution), an agent, or a network scanner. Typical information would be: operating system, vulnerabilities, and open ports.

**Phase 4:** Further network access policy rules are enforced to individual end systems, using assessment data results. The user should be informed about this assessment and should be given the opportunity to remediate if not in compliance with appropriate security policies.

The following sections will detail the technologies critical to supporting a phased NAC implementation.

Detect & Authenticate

Everyone should be able to access the network anytime/anywhere and the network should react dynamically and automatically according to the rules/guidelines for the device and/or user connecting.

In order for this to occur you need to know who is connected to the network and where they are located. Manual documentation of the network should become unnecessary. With NAC, you should be able to realize a self-documenting network.

"How can an end system or user be identified?"

MAC and IP addresses are the most commonly used methods for identification, but they can be changed in less than two minutes and are therefore only suitable to a limited extent. Actually, the identification of an end system goes hand in hand with its authentication. The same mechanism that is used for authentication is often also used to identify the end system.

However, the question you need to ask before deciding on any method is: “What authentication is supported by the end system?”

There are many technical methods that can be leveraged for authenticating end systems and/or users. A comprehensive NAC solution should be able to support multiple methods:

- 802.1X port based authentication (via RADIUS)
- MAC based authentication (via RADIUS)
- Web based authentication
- Static port/MAC configuration
- Dynamic port/MAC configuration (SNMP)
- Kerberos snooping

Other context such as host name or IP address can also be used for identification purposes. This can be very effective and helpful, especially for non-desktop systems.

**802.1X**

The most secure authentication method is the detection of end systems at the network switch port using 802.1X authentication. This requires particular capabilities on the switch, the client, and the local authentication entity (RADIUS server). 802.1X also allows for the authentication of both the end system and the user (either separately or as a combined entity).

There are situations where the 802.1X authentication method is not appropriate. Some end systems may not support or do not contain an 802.1X supplicant (the software agent for authentication). Examples of devices not supporting 802.1X might be older printers or IP video cameras. Also, there are some network switches that do not support 802.1X. Finally, guests may not be configured correctly, based on the corporate IT standards, to be authenticated via 802.1X.

Companies often have heterogeneous networks that may support partial or no authentication. The goal here is to implement improved technology wherever possible. However, a complete replacement of the network is usually a cost-prohibitive proposition. The goal should be to ensure any new network switches support 802.1X as well as multiple individual authentication sessions per port. They should also support different authentications for multiple end system types allowing per port flexibility (e.g., VoIP phone plus PC or mini-office/cable switches).

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Benefits</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| If all requirements are fulfilled, 802.1X offers a very scalable and dynamic identification with a high level of security at the switch port. | • Standard for current systems  
• Centralized administration  
• Real time detection  
• High level of security  
• Good scalability  
• Additional information (user, host) | • Many requirements  
• Subsequent upgrade expensive |

**MAC Based Authentication (via RADIUS)**

MAC based authentication uses the same basic elements as 802.1X. The difference is the abandonment of certificates and/or registration data. The switch uses the end-system’s MAC address as a replacement for the user name and verifies this with the RADIUS server. This method can be used in networks that support 802.1X to verify all end systems with the RADIUS server without the “supplicant”. A common implementation strategy is to start off with the MAC based authentication method for the entire network and later migrate to 802.1X for the end systems where there is support. This method only offers a limited level of security and should only be used in combination with restrictive authorization. Additional information, like the user name, is missing and subsequent authorizations will be tied to the hardware address of the end system. An advantage of this method is the centralized administration of all users via the RADIUS service.
Conclusion | Benefits | Disadvantages
---|---|---
This method is a solution for special end systems. It is better than static port/MAC assignment since dynamic and scalability are the same as for 802.1X. | • Standard for current systems • Centralizes administration • Real time detection • Good scalability | • Many requirements • Low security • Additional information is limited

Web Based Authentication

This method of authentication relocates the “supplicant” to a web portal to which a user has to login. With this method, guests and end systems not fulfilling the necessary requirements for network access can also register to the network. Guest access only requires a very basic registration. An elegant example of secure guest access is sponsored registration, where existing users agree to compliance of their guests. With this method, the IT organization can easily audit who has sponsored each guest accessing the network without having to get involved in providing temporary credentials. In this example, a default policy is enforced, only allowing connection to a web portal. Once authentication at the web portal is successful, further services can be allowed. It is interesting to note that many solutions do this via dynamic VLAN configurations. This separates the end system from the production network, but usually does not define any restrictions within the VLAN. VLANs are not sufficient security containers. VLANs are meant to be logical broadcast containers.

A well architected NAC solution may use a different approach. Traffic can be classified by the network switches based on OSI layer 2 through 4 information in the packets, allowing enforcement of firewall-like rules to individual traffic flows in the network. This will be further explained in the Authorization section.

Conclusion | Benefits | Disadvantages
---|---|---
This method is more an addition than a complete authentication method. It simplifies the administrative effort for guests and allows access to older devices. | • Centralized administration • Real time detection • Good scalability | • Additional service administration • Additional registration portal • Unsecure quarantine

Static Port/MAC Configuration

The manual allocation of MAC addresses to a switch port has become a standard security practice. But as the name indicates, static port/MAC configuration is neither automatic detection nor secure access. Since many organizations still use this configuration, it is highlighted here as an extremely weak, but inexpensive, method of access control.
Conclusion Benefits Disadvantages
The cheapest, but the least useful solution for NAC.

Cheap
Works for every switch

High administrative effort
No centralized management
Low security
No additional information

Dynamic Port/MAC Configuration (SNMP)
There are a lot of niche-solutions on the market that try to replicate the process of detection and authentication via SNMP. Some organizations prefer using this method if no directory or RADIUS framework is available. The advantage is clearly the out-of-band management, compatible with all SNMP devices, but this compatibility is also one of the main problems. Many vendors deliver imprecise or faulty information via SNMP where a correct outcome cannot be assured. In addition, authentication via SMNP does not conform to any standards and is not real-time capable since SNMP requests are sent in polling intervals.

Queries via SNMP can lead to excessive load on routers and switches, and in the worst case can crash an infrastructure device itself. In regards to security, the process of port/MAC configuration is managed dynamically. With this, knowledge exists identifying where an end system was located during the last query. An often used counteraction is disabling the port or reconfiguring the port VLANs. Neither of these options gives the user any visibility as to why access to the network has been denied. Also, VLAN reconfigurations often run into problems if DHCP is in use and the client does not ask immediately for a new address. Due to the very limited security in combination with the several other problems and the administrative effort involved, this method should only be used in very small environments, and only if 802.1X is not an option.

Kerberos Snooping
The Kerberos protocol is used for authentication in a network. Typically for, but not limited to, Windows Active Directory domains (Novell NDS uses it as well and it is often used in Linux environments). Kerberos snooping reads encrypted data traffic and can identify if a system has successfully logged on to a domain. Kerberos delivers the username and the host name as identification attributes.
The advantage of Kerberos snooping is that the only requirement is the usage of the Kerberos protocol. The identification and authentication is detached from the switch and can often be implemented without any major intervention. The disadvantage is the need for an in-line appliance similar to an Intrusion Detection System to read the relevant communication. The appliance offers a lot more functionality than a standard 802.1X implementation on a switch. Such a solution is possible for environments needing a higher level of firewall-like security and also when no other possibilities of identification are available. Such an appliance is typically used in the distribution layer of a tiered network and can also monitor WAN transitions like VPN access. This solution allows a quick implementation of NAC without investing in intelligent access switches.

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Benefits</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Flexible, easy, and fast to implement solution. Has to be in-line and is hard to roll out for a complete environment due to costs. | • Fast implementation  
• Centralized management  
• Flexible authentication also for layer 3 networks  
• Offers additional information | • No standard  
• Kerberos environment necessary |

The authentication methods above are the most common, but not necessarily the only methods. To decide which method might be the best for a specific organization, some analysis can help:

- Which of my end systems can be authenticated with which method?
- Can problematic end systems be locally limited (e.g., industrial facilities)?
- What requirements does my network offer for authentication?
- Which systems that might be problematic today can be adjusted in the future?
- Which authentication methods will still be applicable in the future?
- Does more than one end system need to be authenticated on a single port (e.g., a VoIP phone and PC)?
- If more than one end system has to be authenticated, can this be done via different methods (e.g., 802.1X and web)?

In most cases, a combination of methods is necessary to ensure full NAC functionality across the network. Even if a large portion of end systems can be authenticated via 802.1X, an in-line appliance capable of a variety of authentication methods would offer strategic points to ensure more NAC coverage.

**Assessment**

A strong integration of the registration process into the assessment of an end system is still not very common. The registration process is an important component of NAC implementation. Standards for assessment frameworks are the Microsoft (Network Access Protection) and TNG (Trusted Network Connect) frameworks. The IETF is also working on this but doesn’t have a completed framework at the moment. The function of assessment goes beyond the switch port and tries to assess the end system itself. Assessments, or health-checks, can be separated into two methods:
Agent-less:
Network Based - a network scanner scans the end system remotely (over the network)
Applet Based - a java applet is used to launch assessment functions on the end system (web browser based)

Agent-based:
Thin Agent - a temporary agent (can be loaded and unloaded on the end system using various vendor-specific techniques)
Fat Agent - a persistent suite of assessment software with firewall and host intrusion detection established on the end system

During an assessment, end systems are checked for compliance and/or vulnerabilities. This also includes testing the end system embedded firewall and other applications for vulnerabilities.

Determining which assessment method is the most appropriate for a particular environment is based on what you are trying to check and what possibilities the end system allows. It would obviously be a challenge to install an agent on a printer or telephone. On the other hand, a network scanner may run into problems with a local anti-virus scanner when trying to scan for current virus signatures.

The assessment duration and load on the network is also very different for each method. A network scanner scans the network and therefore can cause more load and requires more bandwidth. An agent relocates this load onto the client and only requires local resources until the final report is sent to a centralized location. Local resources required for fat agents can be extensive since they often work via self enforcement to also serve as personal firewall and/or host intrusion prevention systems. The required time for scanning with any of these methods is difficult to measure as it depends on the tests and their intentions. A quick scan for the local firewall process is of course easier and faster than a more comprehensive scan with tests for vulnerabilities on thousands of Layer 4 ports.

An extensive assessment can not only provide health status information about the end systems, but also additional data for inventory and auditing purposes.

Agent-less

The extent of the end system tests partly depends on the software used for the assessment, but is also limited by what can be done off-box. There is a large market for vulnerability scanners offering a wide array of programs that are only designed for this and are continuously updated with new test sets.

Generally an assessment includes the following steps (in no particular order):

1. Availability & identification – Ping, DNS lookup
2. Portscan – TCP/UDP
3. Vulnerability identification
4. Vulnerability exploits

Each of these steps should be separately configurable and one should be able to use the results for any following step. For load and performance reasons it makes sense to only scan open ports for vulnerabilities. Some network scanners can also connect to the client itself (with user name and password) and run local tests on the client. Care is required when performing a vulnerability scan since this can cause a crash of the end system.

The disadvantage of this method is the accuracy of the results, since on one hand you are only able to check for known vulnerabilities and on the other hand services and versions cannot be accurately identified via remote communications through the network. Another issue is the increased load (caused by the scan) on the scan server itself. It is actually quite unrealistic to regularly scan thousands of end systems with a single server since this will not scale well. An advantage of this method of assessment is the extent of the tests - which are usually greater than an agent could provide. In addition, in an environment with guests you don’t need to force them to install any software.
The major advantage of this method is the capability to scan end systems that don’t allow any agents, which of course increases the number of devices included in a NAC implementation.

### Conclusion

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Network scans automate many manual tests and are performed by centralized servers within the network. Especially recommended if agents are not an option. | Fast implementation  
Frequent signature updates  
Extensive tests  
Detailed client information  
High end system compatibility |
| Cost (initial and maintenance)  
Scalability  
Features  
Administration  
Security Value  
Additional Benefits / ROI |
| Limited scalability  
Time consuming scans  
Network load |

### Agent-based

An agent is a standalone piece of software that runs on an end system and provides information about the health of an end system and in some cases also works proactively against threats. The big advantage of an agent is the option to request and check all data on one system. But there are also disadvantages with this method. Since an agent has to be installed on the end system, there may be limitations in the coverage capability within an enterprise network environment.

In areas with multiple operating systems and applications, extensive adjustments of configurations on the client may be necessary and often are not even considered as an option. The agent also has to be very “social” and has to be able to communicate with its environment. This can cause problems in a multi-vendor environment. Most NAC vendors also offer their own agent to strengthen their NAC solutions and to restrict any integration with other solutions.

There has been some work to design better interoperable frameworks to include multi-vendor agent options. Microsoft offers its Network Access Protection (NAP) as an interface between agents and NAC on the operating system itself. Generally one should consider the sustainability and compatibility to remain flexible for any future decisions involving a NAC deployment.

An assessment agent typically offers the following information:

- Is the firewall up and running?
- Is an antivirus program installed and are the signatures up to date?
- What operating system is running?
- What is the patch level of the system?
- Is there a connection to the agent?
- What software is installed?
- What processes and/or services are running?

The possibilities are almost indefinite, but specific tests add complexity since the agent first has to learn what should be tested and how to differentiate between good and bad. An agent is able to perform an assessment and provide the results quicker than other methods. It also relocates the majority of the load to the end system. This makes the agent-based solution more scalable for larger network environments. In some cases the agent can also perform auto-remediation like turning on the local end system’s firewall. Guests are also easier to manage with the use of dissolvable agents, where the agent installs in RAM on the end system and “dissolves” after the next restart of the system.
## Conclusion

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents can do it all (almost) but not on every end system. Actions can be run locally on the client and load and scalability are ideal.</td>
<td>Direct access to client information</td>
</tr>
<tr>
<td>• Proactive actions</td>
<td>• Very good scalability</td>
</tr>
<tr>
<td>• Very good load balancing</td>
<td>• Very short scan time</td>
</tr>
</tbody>
</table>

Obviously there is not just a single assessment solution for all end systems. The best approach would be agent where possible and a network scan where needed. Both methods supplement each other, and in environments with a high level of security it sometimes even makes sense to use both at the same time. Another advantage, apart from the information about the security level of the end systems, is extensive documentation of all network devices. This advantage is even bigger if the NAC solution provides open interfaces for all kinds of data.

## Authorization

After detecting, authenticating, and assessing an end system, a well architected NAC solution can leverage the information learned to perform an authorization for the end system to access the network and specific services.

The authorization process applies all the rules planned during the preparation phase of a NAC deployment. As discussed previously, there are multiple options available regarding authorization of services for end systems. These options may be dependent on the performance of the network and in particular the NAC solution’s capabilities. Additionally, choice of authorization enforcement options also depends on the required level of security as well as the design of the infrastructure itself. It is important to know if more than one end system needs to share ports or if devices, users, ports, or individual traffic flows need to be considered.

Some questions to ask are:
- What level of granularity do you need? On port-, user-, device-, traffic-layer?
- Should everything be denied by default and only permitted case by case? Or vice versa?
- How is authorization of multiple devices on the switch port handled?

## (Port) VLAN Allocation

This is the most common and also standardized (RFC3580 via 802.1X and RADIUS) method for granting access rights. Every port is by default in a guest, or so called quarantine-VLAN. After successful authentication and assessment, the authorization moves the port into a production VLAN. This is a very common method since many switches support VLANs and it is an easy way to form separate isolated groups. However, this method has its flaws. A VLAN is not a security container and it also is not really scalable as the number of VLANs used in a network is limited. The extent of administration does not scale, the more VLANs, the more IP subnets, the more IP router configurations are required.

Regarding 802.1X and DHCP, an end system must be informed via its "supplicant" that it is in a different VLAN and needs to request a different IP address. Without this capability, issues can arise when changing anything in the VLANs without 802.1X (e.g., via SNMP), and might even cause a loss of connectivity. Some vendor workarounds consist of turning the port on/off but this causes communication issues for other devices/users (e.g., VoIP telephones) when using the same switch port and actually just one device had to be authorized. Multiple clients using one switch port is always a challenge. Some solutions provide the possibility that one of the two devices (generally the phone) can “tag” its communication data with the matching VLAN ID. This allows the switch to differentiate between the two devices. This solution is not optimum since the users/devices should usually leave it up to the network to assign VLANs.
Just allowing one device per port is often not an option and is expensive. Traffic cannot be distinguished and classified, and only a classification for an entire port is used. Port VLAN allocation offers a compromise, but the weaknesses have to be considered when planning the project.

<table>
<thead>
<tr>
<th>Conclusion</th>
<th>Benefits</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| This method is widely spread and fulfills most requirements. A disadvantage is the administrative effort during the planning as well as during operations. There are limitations when having more than one system per port. | • Integrated in most switches  
• Logical isolation from the network  
• Standardized | • Issues with more than one end systems per port  
• Partially extensive configuration |

**Policies**

Policy-based networking and NAC enable a dynamic firewall capability right at the switch port in the network. Policies define what is allowed and not allowed on the network, what priority a device, user, or application can have on the network, and how much bandwidth each are allowed to use. With policies you have the capability of distinguishing between different systems and services, and there is no need for separation with VLANs. In addition to the authorization, traffic can be classified through many characteristics and can be treated individually.

Typical examples:

- DHCP at the user port is not allowed
- HTTP access to a quarantine/remediation server is always allowed, and any further access only after successful assessment
- Legacy protocols like IPX or unusual traffic are detected directly at the switch port
- Applications like Skype or P2P can be limited
- SIP traffic is labeled with the correct quality of service information
- Single flows can be pushed to other VLANs without the client noticing
Although policy enforcement offers seemingly endless opportunities and very high visibility, it is important to know beforehand what is allowed and what is not. This can be simplified through roles and service based policies.

**Disabling Ports**

Disabling ports as an authorization technique is a less-specific approach than enforcing communication policies. Disabling a port disconnects the end system from the network, but there is no possibility of later remediation. It is also impossible to find out if the end system is still connected to the port. To find this out, the port often is enabled again after a short period, checked, and then disabled again. If this isn’t done, a malicious attacker might shut down the entire network by disabling one port after the other.

With this method it is impossible to manage multiple devices on one switch port. At least every switch in the market offers this method, which allows heterogeneous deployments, but the disadvantages typically outweigh this availability. A method that doesn’t even offer the possibility for dynamic remediation is not advisable. It is still used in some small, out-of-band solutions with dynamic port control via SNMP or Telnet/SSH, but should not be an option for typical enterprise deployments.

---

802.1X and other authentication methods are generally used in combination with RFC3580 (Port/VLAN allocation) or policies, if available. Sometimes in-line appliances are used for enforcing policies if the network doesn’t support this capability embedded in the switches. This is also an option for central WAN transitions, especially if access to the infrastructure of remote sites is not available.
Remediation

NAC must have the function of remediation fully integrated into the solution. Without options for remediation, a NAC solution could end up preventing significant numbers of (and possibly all) end systems from connecting to the services they require to maintain business continuity and productivity.

Remediation is the process of supporting end systems to reach the required level of compliance and to then offset restrictions to the network. To minimize the manual remediation process, problems with end systems and user actions should be solved automatically or by the user rather than forcing involvement of the IT helpdesk.

Automated remediation is possible with an agent, since changes in configuration or even services have to be installed (e.g., the firewall) most of the time. In some cases a software management solution can be triggered from the NAC solution to solve the issue.

The most common solution for manual (end user-driven) remediation is a specific remediation web server to which the users are redirected. The advantage of this is a centralized management of the available remediation process, with execution distributed to the end user community.

Important content of a web portal:
- Information about the status of the end system: in quarantine, allowed on the network, etc.
- Specifications about the end systems violation: firewall disabled, outdated signature base, etc.
- Details to solve the issues: enable firewall, contact update-server, etc.
- Information about accessible services: Microsoft update-server, etc.
- Link for re-connection after following the instructions.

Remediation should be automated and minimize user intervention. These systems should only allow administrator access to make sure no additional software can be installed. The better the remediation process, the less additional administrative work load, since most of the troubleshooting can be redirected to the agent or the user.

Questions:
- Who is responsible for the remediation? An agent, the user or the administrator?
- How long does the remediation and the reconnection take?
- Is the remediation portal accessible for everyone?
- Can the portal be adjusted for language, corporate identity?

Monitoring

Up to now the discussion has focused on assessment of end systems in the pre-connection phase. But who can guarantee that changes aren’t done to cause the end system to fall out of compliance after successfully connecting to the network? Tools for a continuous monitoring/assessment are often in place in addition to the recurring pre-connect assessment. Depending on the method, different intervals for post-connection assessment can be used. An agent or a remote scan of an end system can perform continued assessment at a specified interval rate.

The NAC solution should also include a general variety of configuration options to meet the requirements of the network. The chosen NAC solution should work flexibly but based on templates to keep administrative effort at a minimum and simplify troubleshooting.

Some parameters to consider:
- Should systems be assessed every time they connect?
- At what interval should systems be re-assessed (e.g., every week)?
- At what interval should the clients report their findings?
- Can the clients remain connected during the assessment, or should they be quarantined by default?
In addition, NAC is a perfect supplement for behavior and anomaly-based security solutions. These solutions generally evaluate network communications flow data and detect Layer 3-7 attacks but are not able to apply any mitigating action in the actual communication infrastructure. This kind of monitoring can be integrated into a well architected NAC solution to provide granular and effective post-connect protection. Another option is the combination of an Intrusion Detection System (IDS) and a NAC solution to detect attacks and also have an effective automated response system.

The more open a NAC interface is, the more security solutions can use this interface and the greater the value.

Beyond Network Security

Security may not be the main driver for an IT project. Below are some additional benefits (beyond network security) that a well architected NAC solution can provide.

**NAC and VoIP**

Voice over IP (VoIP) itself is already a challenge for every network, especially in larger environments where localizing and prioritizing mobile end systems and convergence endpoints can be difficult and complex. NAC can help simplify this process by providing information about the infrastructure in real time. With policy enforcement, NAC can also support the process of prioritizing different end systems at the switch port. A major issue with VoIP phones is the localization in real time (e.g., for locating a user once an emergency call has been placed). There are integrations of NAC and VoIP Management services available today that can provide this location information. The automatic call diversion and reconfiguration depending on the location of that particular phone is another advantage of such integrations. Additionally, NAC can assist in proactively detecting IP phones as part of the access control process.

**NAC and the Security Infrastructure**

Every company uses a firewall; some even have Intrusion Detection/Prevention Systems (IDS/IPS), application layer gateways, or even Security Information and Event Management (SIEM) systems. Usually these systems detect attacks to the network very well, but there is always the restriction that actions can only be taken on that respective system. A firewall for example can detect an unauthorized access attempt and can block this, but it can’t perform any actions against the relevant system. A well architected NAC solution can assist by reporting identity data, like location, user, and security level to another system, which gives the administrator a centralized view of all the data. It also offers the most effective action if an end system shows unusual behavior, is not compliant, or even starts an attack; NAC can restrict any access rights from the end system.

**NAC and Virtual Servers**

Clusters and virtual servers in the network are more popular than ever, especially since a dynamic relocation of software onto hardware provides more efficiency and flexibility. However, most networks do not offer that level of flexibility, and any configurations (e.g., data prioritization) require manual administration. It is even more difficult to relocate virtual systems automatically (e.g., during a hardware crash). With its localization of servers, a well architected NAC solution offers an easy option for automating reconfigurations of the network and with that helps the network to adjust to the typical drag-and-drop behavior.

**NAC and the IT Helpdesk**

As soon as problems occur in the network they need to be localized. NAC offers a centralized database, holding information about the identity, level of security, and location of users. Ideally NAC should also offer reports for the assessment information and provide historical data for all end systems. The addition of policies takes this even further and can solve issues right at the source, since problems can be detected and mitigated at the switch port.

**Summary**

A NAC project does not have to be complex and difficult. NAC deployments can be broken down into logical steps or phases and incremental benefits can be quickly realized throughout the implementation process. The success of a NAC project really depends on the right start. The more information that is available and the better the policies are defined, the easier the actual implementation will be.

To learn more about how Enterasys provides a well architected NAC solution, visit us at [www.enterasys.com](http://www.enterasys.com).
Appendix

The following attachments highlight some examples and checklists for various NAC deployment scenarios. A demo environment for testing is always advisable to evaluate potential solutions before implementing into a production environment.

Attachment A: Example Checklist Roles/Rights

<table>
<thead>
<tr>
<th>Group</th>
<th>Role</th>
<th>Rights</th>
<th>Resources</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>Sales</td>
<td>SAP, Mail, Internet</td>
<td>Sales server</td>
<td>Sales floor</td>
</tr>
<tr>
<td>Marketing</td>
<td>Sales</td>
<td>SAP, Mail, Internet</td>
<td>Marketing server</td>
<td>Marketing office</td>
</tr>
<tr>
<td>Administrator</td>
<td>Allow all</td>
<td>Unrestricted</td>
<td>Unrestricted</td>
<td>Unrestricted</td>
</tr>
<tr>
<td>Guest</td>
<td>Guest</td>
<td>Internet</td>
<td>None</td>
<td>Conference rooms</td>
</tr>
<tr>
<td>Quarantäne</td>
<td>Quarantine</td>
<td>Only remediation</td>
<td>None</td>
<td>Unrestricted</td>
</tr>
</tbody>
</table>

Attachment B: Example Checklist Infrastructure

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Location</th>
<th>VLAN</th>
<th>Authentication Options</th>
<th>Assessment Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>Sales</td>
<td>2</td>
<td>802.1X, WPA, MAC</td>
<td>Agent, Netscan</td>
</tr>
<tr>
<td>PC</td>
<td>Marketing</td>
<td>3</td>
<td>Kerberos, MAC</td>
<td>Agent, Netscan</td>
</tr>
<tr>
<td>PC</td>
<td>Administrator</td>
<td>4</td>
<td>802.1X, WPA, MAC</td>
<td>Agent, Netscan</td>
</tr>
<tr>
<td>Server</td>
<td>Sales</td>
<td>5</td>
<td>802.1X, MAC</td>
<td>Agent, Netscan</td>
</tr>
<tr>
<td>VoIP</td>
<td>Sales</td>
<td>6</td>
<td>802.1X, MAC</td>
<td>Netscan</td>
</tr>
</tbody>
</table>

Attachment C: Example Checklist Assessment Checks

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Role</th>
<th>Type</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>Sales</td>
<td>Agent</td>
<td>Firewall, Antivirus, Patchlevel</td>
</tr>
<tr>
<td>PC</td>
<td>Marketing</td>
<td>Agent</td>
<td>Firewall, Antivirus, Patchlevel</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN</td>
<td>Agent</td>
<td>Firewall, Antivirus, Patchlevel, Malware</td>
</tr>
<tr>
<td>Server</td>
<td>Sales</td>
<td>Netscan</td>
<td>Portscan, Vulnerability Scan, Password Guessing</td>
</tr>
<tr>
<td>VoIP</td>
<td>Sales</td>
<td>Netscan</td>
<td>Portscan, Vulnerability Scan (all)</td>
</tr>
<tr>
<td>Laptop</td>
<td>Guest</td>
<td>Netscan</td>
<td>Portscan, Vulnerability Scan (except DoS)</td>
</tr>
</tbody>
</table>

Attachment D: Example Checklist Reporting

<table>
<thead>
<tr>
<th>Information</th>
<th>Time schedule</th>
<th>Recipient</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated Systems</td>
<td>Daily</td>
<td>Administrators</td>
<td>With definition of the method</td>
</tr>
<tr>
<td>Quarantine Systems</td>
<td>Daily</td>
<td>Administrators</td>
<td>With reasons</td>
</tr>
<tr>
<td>Top 10 Vulnerabilities</td>
<td>Weekly</td>
<td>Security Officer</td>
<td>Forward to Executive team</td>
</tr>
<tr>
<td>Number of VoIP Phones</td>
<td>Monthly</td>
<td>Administrators</td>
<td>By vendor</td>
</tr>
<tr>
<td>Guest Accesses</td>
<td>Weekly</td>
<td>Security Officer</td>
<td>Duration, sponsor information</td>
</tr>
<tr>
<td>Device by Location</td>
<td>Monthly</td>
<td>Administrators</td>
<td>Separate by device type</td>
</tr>
</tbody>
</table>
Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com