

Access Controls in NAC

Network Access Control, NAC, is based on a simple idea: what you can do on a network is a function of who you are and the state of your end-point security. To build a NAC solution, you have to bring together three specific security components under a common management umbrella. The two starting components for NAC are authentication (identifying who the user is) and environmental information (identifying, among other things, the state of end-point security on the user's device). The third, and most critical, component, is enforcement: making sure the user does, in fact, only go where they have permission to based on NAC policy.

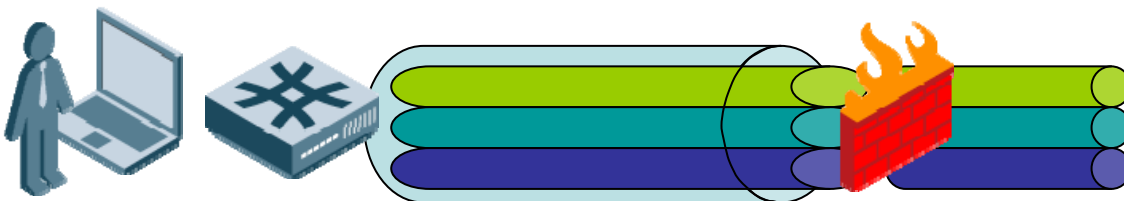
A spectrum of choices exists in access control methods, ranging from a simple "go/no-go" type of control up to full stateful firewall rule sets. In the middle are the two most commonly used access control techniques: VLAN segregation and packet filtering access control lists (ACLs).

VLAN Segregation

VLAN segregation is a common access control technique in NAC designs. With VLAN segregation, users are placed onto VLANs, which are segregated by some access control device, typically a firewall. For example, one VLAN might be for employees, one for guests, one for VoIP phones, and, of course, one for quarantined users in need of remediation. The firewall policy is static in the sense that everyone on a VLAN has the same policy. Thus, all the users and devices on a particular VLAN have the same access.

VLAN segregation is a coarse-grained access control technique, which may be perfectly acceptable in a NAC deployment. In addition, VLAN segregation is attractive because it is widely standardized and widely implemented. This makes it easy for someone to design a NAC architecture, and easy for everyone to understand the details of the deployment.

The picture below shows a rough idea of how VLAN segregation works. A user is placed on one of three VLANs based on the NAC policy. The VLANs are maintained separately from each other in the switching infrastructure, and eventually connect via some firewall responsible for controlling access and possibly even routing between the VLANs and other parts of the corporate network. In this picture, the firewall is primarily responsible for controlling the user's access to the rest of the network, although the policy on the firewall is not user-specific, but common to everyone on the VLAN.



Issues in VLAN Segregation

While VLAN assignment works fine in small networks, the collective experience of the Interop Labs team in doing actual NAC deployments has shown that many networks can't use VLAN assignment.

Sometimes the network is too large and too distributed, which may make it difficult or impossible to propagate VLANs between buildings and sites, especially remote offices. Other times, VLANs are already being used for a different purpose and can't be re-used for security boundaries without causing massive disruption and redesign. And, of course, some NAC projects have a goal of a finer-grained access control than VLANs can provide, or would like to provide per-user access controls to keep quarantined or guest users from attacking and infecting each other.

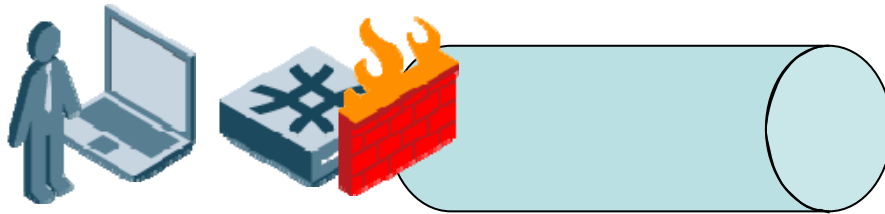
Of course, none of these mean that VLAN-based access controls are not good. In a single site network where the main purpose of NAC is quarantine of non-compliant users, VLAN-based access controls have become the de-facto standard for deployment and are often the preferred approach. The simplicity and wide support of VLAN-based access controls make them more compatible and less expensive to add to existing networks.

Packet Filtering Access Control Lists (ACLs)

The other commonly discussed NAC access control is Packet Filtering ACLs. While this can be combined with VLAN segregation, for the sake of simplicity we'll discuss this assuming you are using one or the other.

Packet Filtering ACLs are the great-grandparents of today's modern firewalls. A contemporary firewall follows TCP connections (is "stateful"), has application layer gateways, and generally provides an extremely fine-grained and controlled access control between two networks. Packet Filtering ACLs (sometimes called "stateless") are less sophisticated than firewalls, but are often sufficient for the requirements of an enterprise NAC deployment.

Packet Filtering ACLs have another huge advantage over firewalls: they're already implemented in most existing enterprise-class switches. This means that a NAC deployment can apply these relatively simple access controls at the edge of the network without disturbing any of the existing topology, creating bottlenecks, or requiring additional capital investment.



Packet Filtering ACLs are normally applied on input to the switch from the device, which is sufficient to control communications in both directions. Here is an example of an ACL we used in the Interop Labs for our quarantine network:

```

permit udp to DNS-Server 53      ! let DNS queries work
permit icmp to any               ! let any ICMP (ping, etc.) work
permit ip to Quarantine-Server  ! let talk to Quarantine server
permit udp to 255.255.255.255 67 ! let DHCP an address
permit udp to DHCP-Server 67    ! and talk to DHCP server
deny ip to any                  ! and block all else

```

Anyone studying this can see that this is not as sophisticated or as controlling as a full firewall – but it is likely sufficient to help quarantined users get their software updates and keep them from causing trouble on the corporate network. Switches usually have a limited amount of capacity for ACLs, so keeping them short is often a requirement to stay with current hardware. Most of the wireless and wired network equipment in use in enterprise networks is able to use ACLs to control end-user policy. Equipment will typically fall into one of two camps.

The majority of equipment all work by having ACLs pre-loaded into the equipment by the network manager. Then, the NAC policy server simply points to an ACL when responding to the RADIUS authentication request and this ACL is applied to the end user. For example, on our Aruba wireless equipment, we defined four access control lists to differentiate between employee, quarantined, and administrative users and devices like printers and VoIP phones. When an employee connects, the NAC policy servers would send a specific RADIUS attribute with a pre-determined value (such as 1, 2, 3, 4) for the ACL that should be applied to that user. It is not necessarily simple to do this, because there is no commonly-accepted way to send down the choice of ACL. For example, on Cisco switches, one type of RADIUS attribute (Filter-ID) is needed, while on Cisco's wireless equipment, a different RADIUS attribute (Airespace-ACL-Name) is needed. In some cases, the pre-loaded ACL might include other information, such as QoS settings and a VLAN selection.

The rest of the ACL-supporting equipment requires the ACL to actually be generated on the policy server and pushed to the switch. For example, on the HP wired and wireless equipment in the Interop Labs, we send down the full ACL, not just a pointer. Although this is a less popular approach, it offers a different way to manage security in a more dynamic fashion. We found that most policy servers can store and send pre-built ACLs (sometimes just called "text blobs") to switches, but that no policy server was dynamically generating the ACL on-the-fly.

One final twist on the question of Packet Filter ACLs versus VLAN segregation is to recognize that some NAC deployments will use both at the same time. For example, in the Interop Labs, we used a single VLAN for all "employee" traffic (employees, whether quarantined or not) but separate VLANs for VoIP phones and guest users.