

The Importance of Secure Guest Access

The Cisco® NAC Appliance helps organizations secure guest access to corporate networks, ensuring that guest and visitor traffic remains segregated from internal networks and assessing incoming computers for threats that may affect network availability and security. The Cisco NAC Appliance offers centralized guest access management and enforcement for wired and wireless users, and can integrate easily with wireless solutions, third-party guest access portals, and billing providers.

The Enterprise as Public Hotspot

Enterprise networks are one of the most important hotspot destinations for today's business travelers. With the growth of wireless networking, contracting, and outsourcing, offering visitors Internet access has become a necessity. Providing guest access requires an organization to maintain the security of network resources while minimizing the IT support required for the service. Specifically, the business challenges to offering guest access include:

- Restricting visitor access to the Internet only or a subset of internal resources, depending on the type of guest
- Seamlessly supporting wireless and wired access
- Centralizing management and control
- Enforcing security, corporate, or governmental policies on guest users and devices

These business challenges, in turn, translate to several technical requirements for an optimal and secure guest access solution:

- **Usability for guests:** Guests should not need to reconfigure their laptops or download an agent; authentication should be Web-based.
- **Usability for the enterprise:** Solutions should be "plug-and-play", supporting corporate proxy settings and overlaying onto the existing network; non-IT staff should be able to set up and manage guest user accounts.
- **Flexibility for the enterprise:** Solutions should allow for splash screens and Web content that differs by location and device.
- **Manageability for the enterprise:** Administrators should be able to conduct a full audit of the location of guest users, their MAC address, IP address, and username; and should be able to ration bandwidth to ensure network performance for employees.

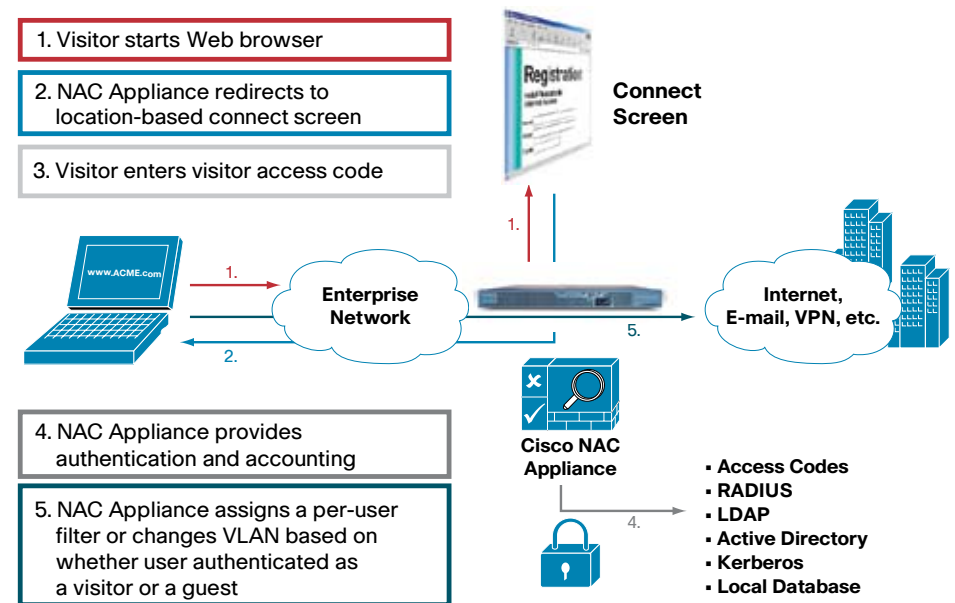
- **Control for the enterprise:** Solutions should ensure that legal requirements are fulfilled, in the form of a customizable disclaimer or Acceptable User Policy (AUP) that must be accepted as a condition of access.

Cisco NAC Appliance for Secure Guest Access

The Cisco NAC Appliance is the keystone of a robust secure guest access solution. As a product that enforces policies before granting access to the network, the Cisco NAC Appliance can be used alone, integrated with a pre-built solution from Cisco Advanced Services and other third-party guest access portal partners, or fully customized using the appliance's open API.

The basic guest access process is illustrated in Figure 1.

Figure 1 Automate and Control Visitor Internet Connections



Used alone, the Cisco NAC Appliance accommodates visitors by creating guest user accounts through its Web-based interface, the Cisco NAC Appliance Manager. Guests are assigned to the "guest" role, through which administrators can limit bandwidth and restrict resource access in a highly detailed way.



When combining the Cisco NAC Appliance and guest access portal applications, such as those offered by Cisco Advanced Services or VisitorNetworks (www.visitornetworks.com), enterprises benefit from full account lifecycle management and enhanced usability tools. Any sponsoring employee can create login credentials for a guest by using a centralized intranet portal and can view the full lifecycle of the guest accounts created. The NAC Appliance enhances guest access portal applications by permitting the network administrator to:

- Define a guest policy based on the operating system of the incoming device and its location
- Create dynamic filters based on user, IP address, and DNS
- Require the acceptance of a disclaimer or AUP
- Separate guest traffic at Layer 3, using /30 subnet assignments
- Integrate easily with existing Cisco Unified Wireless products

As a third option, enterprises can design their own guest access portal, using the Cisco NAC Appliance as the mechanism for controlling access and enforcing policies. By using the appliance's open API, enterprises can link a guest access solution to other systems, such as temporary badge printers, access key cards, or billing applications.

Figure 2 outlines the three guest access deployment options based on the Cisco NAC Appliance.

Figure 2 Deployment Options for Secure Guest Access

Direct on NAC Appliance Manager	External Guest Hotspot Portal	Custom Application
<ul style="list-style-type: none">• Create guest or any other role-based account• Provide lobby administrator privilege to create accounts only• Locally created on the manager	<ul style="list-style-type: none">• GuestNet Manager• Visitor Networks• Full account lifecycle management• Printing / e-mail account details	<ul style="list-style-type: none">• NAC Appliance has an open API• Create your own application to set up account• Link to systems such as badge printers, etc.
Multiple options ease initial deployment and allow for future integration into existing applications		

Benefits of Secure Guest Access with the Cisco NAC Appliance

Because the Cisco NAC Appliance is primarily a policy enforcement solution, it adds a deep layer of security for guest access. As enterprise networks support more diverse types of visitors, from contractors and consultants to conferences and meeting attendees, securing internal resources and maintaining the operation of the network become even more critical.

Using the Cisco NAC Appliance for secure guest access generates several benefits:

- Reduces initial and ongoing costs by consolidating wireless and wired access for guests
- Greatly increases flexibility in granting and controlling network resources based on visitor type
- Improves the guest experience while reducing IT overhead
- Increases security and network resilience by assessing security posture on incoming devices

Benefits of Cisco

Choosing Cisco for secure guest access takes advantage of the most widely deployed network admission control solution on the market today. Guest networks are evolving into core elements of business productivity, requiring greater flexibility, manageability and, most importantly, control.