Five Crucial Steps to Deploying a Secure Guest Network

Cisco Mobility TV
Cisco Mobility TV

Mobility TV Host
Chris Kozup
Senior Manager, Mobility Solutions Marketing, Cisco

Brian Uffelman
Product Manager, Wireless Networking BU, Cisco
Agenda

1. Guest Access Business Drivers
2. Network Segmentation
3. User Policy Management
4. Guest User Provisioning
5. Login Portal
6. Reporting and Billing
7. Cisco Guest Access Solutions
## Drivers for Guest Network Access

### Providing a Positive Visitor Experience

- Visitor Access for VPN
- Internet Access for Customers
- Contractor Secured Internal Network Access
- On-Site Vendor Demos
- Segmenting Visitors from Subsidiaries

### Balancing the Needs of Guest Users and IT Departments

- Network Integrity and Security
- Customized Access
- Simplified Network Design
- Cost-Effective Deployment and Operations

### Streamlining IT Mgmt. and Control

- Guest Access
The Challenge of the “Guest” User

- Guest traffic should be segmented from the internal network
- Limited internal network access must be extended to guests securely
- “Guest network” must be cost-effective and non-disruptive
- Must not require guest desktop software or configuration
Types of Network Users

Corporate Employees
- Need internal network access
- Can be role based to allow granular access if needs require

Contractors/Consultants
- Need restricted internal access
- Printers
- File shares
- Specific applications
- Device support

Guests Users
- Internet access only
- No need to access internal systems
- Segment access completely

Cisco Guest Access Gives You Control
Guest Access Solution Entities

User

Access
- Secure Catalyst Switch
- Access Point

Network Enforcement
- NAC Appliance
- Wireless LAN Controller

Guest Lifecycle Management
- NAC Guest Server
- Cisco WCS

Sponsor

New!
Components of a Guest Access Solution

- Network Segmentation: IT Admin Function
- User Policy Management: IT Admin Function
- Guest User Provisioning: Employee Function
- Login Portal: Guest User Function
- Reporting, Billing: IT Admin Function
Network Segmentation

**Goal:** Ensure security by segmenting guest traffic from the internal network out to the Internet/DMZ (unsecured) edge

**Requirement:** Ease of network design, configuration and operation. Compatibility with existing network architecture

**Architectural Flexibility to Ease Deployment and Operations**

**VLANs**
- Use of a 802.1Q trunk for switch to AP connection to carry all the defined VLANs (one VLAN per SSID)
- VLAN isolation ceases if there is a Layer 3 hop between WLAN Controller Internet edge

**Tunneling—Ethernet over IP**
- Provides tunneling (encapsulation) of traffic between WLAN Controllers out to Internet/DMZ edge
- Can carry traffic for all guest SSIDs in single tunnel—simplifies configuration and network architecture
- Can traverse Layer 3 networks—simplifies network design
Network Segmentation
Ethernet over IP Tunneling

- EoIP tunnels logically segment and transport guest traffic between access layer and Internet edge
- Original guest’s Ethernet frame maintained across LWAPP and EoIP tunnels
- Eliminates need for guest VLANs across network
- EoIP supported on all Cisco WLAN Controllers
  - Catalyst Wireless Services Module
  - Cisco 4400 Series
  - Cisco 3750 Series
  - Cisco 2100 Series (tunnel origination only; no termination)
  - Cisco ISR WLAN Controller Module
Enhancing Cisco Unified Wireless Guest Access with NAC

Increased Flexibility

- Dynamically provisioned wired guest ports
  Wired ports can be provisioned as “guest ports” at the time the guest logs in (no pre-provisioning of wired guest ports required)
- Improves network scalability
  Centralizing authentication, posture assessment and remediation provides easier visibility to the network administrator

Improved Policies

- Provides new policy options:
  Integration with broader AAA (LDAP, AD)
  Granular access control
  Bandwidth policies
- Added security benefits:
  Network privileges based on user roles/groups
  End-user security posture assessment, restriction and remediation
Considerations for Guest User Policy Management

- What type of Guest Access is Required?
  Wired?
  Wireless?
  Unified Wired and Wireless?

- What are the bandwidth policies for different types of guests?

- How are large numbers of guests provisioned?
Comprehensive User Policy Management

**Time Of Day Access**
- Provision Guest Network Access based on when network usage is required
- Provides granular control over when guests can access network

**Technology Specific**
- Easily deployable universal (wired or wireless) guest access
- Deploying appropriate access per site, location, or network user population

**Per User/Role**
- Extend network access based on the specific user or group
- Granular, role-based access enhances network security
Guest Network Bandwidth Policy Controls

Requirements
- Specify bandwidth limitations and policies by individual user or group
- Allocate resources by specific job function or throughput requirements

Benefits
- Organization’s overall network performance is enhanced
- Increased granularity and control improves network security
## Guest User Provisioning Enhancements

### Considerations Features

- Guest Provisioning Templates: Configure guests using pre-configured provisioning templates
- Bulk Guest User Provisioning: Providing the ability to configure multiple guest users at once

### Business Benefits

- Streamlines guest access provisioning
- Single-click guest provisioning reduces errors made by provisioning personnel
- Templates are defined and uploaded by the network administrator
- No “network knowledge” required to provision guests when locked-down templates are in place
- Reduces time required to provision multiple groups of users Bulk provisioning of multiple
User Policy Management Options

Integrated Device Management
- Web-based management GUI served from WLAN Controller
- Designed for small, single Controller deployments
- Basic user scheduling

Cisco Wireless Control System
- Web-based multi-device management
- Designed for more feature-rich and multiple controller deployments
- Full-featured user scheduling
- Provision users by physical area

Versatile Management for Any Deployment Environment
Deep Dive: Provisioning

Niall El-Assaad
Product Manager
Cisco
Provisioning

- Who should create user accounts?
  Receptionist/Lobby Ambassador
  IT Security
  Managers
  Helpdesk
  Anyone

- Allowing anyone to create accounts provides increased usage and will be just as secure

- Reduced cost
- Full audit trail
- Speed of access
- Ease of use
Creating Guest Accounts

- What details should be captured?
  
  Name
  Company
  Email
  Phone
  Driving license number
  Anything else?

- When should the account be valid?
  
  Allow setting start/end time
  Pre-defined times: 2 hours, 1 day, etc.
  By usage: 120 minutes from login, 60 minutes in a day, etc

- Where should it be used, and what can the guest do?
Delivering the Guest Account Details

Send Account Information via Print-Out, Email, or SMS
User Login Portal

- Login portal is the splash page guest users are directed upon associating to the guest SSID
- User will need to authenticate on this web page before browsing the Internet
- Is a fully customizable web page that typically includes:
  - Web authentication
  - Corporate branding (i.e. logo)
  - Usage agreement
  - Access to some content without authenticating (walled garden)
How to Implement User Login Portal

Simple and Customizable

- Upload an HTML file from the Wireless Control System (WCS) to the WLAN Controller
- The login portal is then served from WLAN Controller or external server

Additional Considerations

- To help reduce help desk calls:
  - Login failure message portal
  - Logout verification message portal
Deep Dive: Reporting and Billing

Niall El-Assaad
Product Manager
Cisco
# Audit and Reports

## Cisco NAC Guest Server Reporting

### Table:

<table>
<thead>
<tr>
<th>Created By</th>
<th>Username</th>
<th>Full Name</th>
<th>Company</th>
<th>Email</th>
<th>Start Time</th>
<th>End Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>nellasaas</td>
<td>niall</td>
<td>nellasaas</td>
<td>cisco</td>
<td><a href="mailto:nellasaas@cisco.com">nellasaas@cisco.com</a></td>
<td>23rd Sep 2007</td>
<td>23rd Sep 2007</td>
<td>active</td>
</tr>
<tr>
<td><a href="mailto:nellasaas@cisco.com">nellasaas@cisco.com</a></td>
<td>niall</td>
<td>nellasaas</td>
<td>cisco</td>
<td><a href="mailto:nellasaas@cisco.com">nellasaas@cisco.com</a></td>
<td>23rd Sep 2007</td>
<td>23rd Sep 2007</td>
<td>active</td>
</tr>
<tr>
<td>alok</td>
<td>john</td>
<td>john smith</td>
<td>acme</td>
<td><a href="mailto:john@acme.com">john@acme.com</a></td>
<td>23rd Sep 2007</td>
<td>23rd Sep 2007</td>
<td>active</td>
</tr>
<tr>
<td>syed.ghayur</td>
<td>sarah</td>
<td>sarah jones</td>
<td>great stores</td>
<td><a href="mailto:sarah@greatstores.cor">sarah@greatstores.cor</a></td>
<td>23rd Sep 2007</td>
<td>23rd Sep 2007</td>
<td>active</td>
</tr>
<tr>
<td>sponsor</td>
<td>paul</td>
<td>paul johnson</td>
<td>big company</td>
<td><a href="mailto:paul@bigcompany.com">paul@bigcompany.com</a></td>
<td>23rd Sep 2007</td>
<td>23rd Sep 2007</td>
<td>active</td>
</tr>
</tbody>
</table>

### Pages:

1. **Sponsor Information**
2. **Guest Information**
3. **Account Information**
Detailed Information

Cisco NAC Guest Server Detailed Report

<table>
<thead>
<tr>
<th>NAS IP Address</th>
<th>Users IP Address</th>
<th>Logged In</th>
<th>Logged Out</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.3</td>
<td>10.10.10.2</td>
<td>23rd Sep 2007</td>
<td>23rd Sep 2007</td>
<td>1:00:00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12:00:00 America/Los_Angeles</td>
<td>13:00:00 America/Los_Angeles</td>
<td></td>
</tr>
</tbody>
</table>
Paying for Internet Access

Enterprise
- Internal chargeback
- Customer reporting
- Data export
- Integration with internal systems

Hospitality
- Credit card payments
- Pre-paid accounts
- Virtual operator support
- Payment management systems
Tracking Provisioning Personnel Activities

- Provisioning Personnel Audit Trail
  
  Tracking the name of the provisioning personnel who created, deleted, or modified guest user profiles or guest user credentials

- Information assists organizations in more accurately tracking guest user provisioning

- Limiting provisioning personnel to a specific WLC or access point (SSID)

- Constraining provisioning personnel to specific wireless LAN controllers or access point SSIDs enhances network security
Cisco Wireless Guest Access Solutions

Basic, Small Deployment
- Wireless LAN Controllers Using Integrated WLC Management

Enhanced, Enterprise-Grade Guest Provisioning
- Wireless LAN Controllers
- Cisco WCS

Advanced Guest Provisioning and Reporting
- Wireless LAN Controllers
- NAC Guest Server

Increased Guest User Security and Control
- NAC Appliance
- Add to Any Guest Deployment
Cisco Unified Wireless Network Guest Access

Summary & Benefits

Summary

- Delivers all components of guest access within wireless infrastructure
- Guest access part of base WLAN Controller feature set
- Integrated network segmentation and flexible access control
- Non-disruptive to existing network
- Flexible management options suitable for single site SMB through largest enterprise deployments
- Streamlined provisioning and guest user portals

Benefits

- Simplifies network design, no overlay network
- No additional cost
- Secure
- Reduces deployment time, simplifies operations
- Ease of operations
- Reduces IT burden
## Choosing the Right Deployment

<table>
<thead>
<tr>
<th></th>
<th>No DMZ Controller</th>
<th>DMZ Controller</th>
<th>DMZ Controller + NGS</th>
<th>DMZ Controller + NGS + NAC Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Segmentation</td>
<td>VLANs</td>
<td>EoIP or VLANs</td>
<td>EoIP or VLANs</td>
<td>EoIP or VLANs</td>
</tr>
<tr>
<td>User Policy Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Provisioning</td>
<td>Yes</td>
<td>Yes</td>
<td>Enhanced</td>
<td>Enhanced</td>
</tr>
<tr>
<td>Number of Sponsors</td>
<td>Limited</td>
<td>Limited</td>
<td>Many</td>
<td>Many</td>
</tr>
<tr>
<td>User Login Portal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reporting</td>
<td>Yes</td>
<td>Yes</td>
<td>Enhanced</td>
<td>Enhanced</td>
</tr>
<tr>
<td>User Security Posture Assessment</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Increased Access Control Granularity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bandwidth Policing</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for 3rd Party Portals, Cisco GuestNet</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Overall Functionality</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Design Complexity</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Wired and Wireless Guest Access
How it Works

1. Visitor starts Web browser and authenticates to guest portal via wired port (i.e., switch port 11)

2. WLC identifies the port as a guest port and assigns the user to a “guest” VLAN (i.e., VLAN 49)

3. WLC segments guest traffic from employee

4. WLC serves up the captive portal (same as used for wireless)

5. WCS provides guest user provisioning, monitoring and logging (same as used for wireless)
Dynamic Unified Guest Access with Cisco NAC Appliance

1. Visitor starts Web browser
2. NAC Appliance redirects to location-based connect screen
3. Visitor enters visitor access code
4. NAC Appliance provides authentication and accounting
5. NAC Appliance assigns a per user filter or changes VLAN based on whether user authenticated as a visitor or a guest

Access Codes
- RADIUS
- LDAP
- Active Directory
- Kerberos
- Local Database