Nomadix Service Engine
Enterprise Guest Access Application

Thursday, January 05, 2012

30851 Agoura Road
Suite 102
Agoura Hills, CA 91301 USA
www.nomadix.com

White Paper 230-1040-001

Introduction

More and more enterprises recognize the need to provide easy, hassle-free Internet access to people visiting their offices, without decreasing the security of their own Local Area Network. Examples of people visiting and in need for a broadband Internet connection are consultants, sales managers and employees from other branch offices. They want to upload / download their email, load the latest information from their file servers or search in their databases for order intake and delivery, thus making their time at your office more productive. The solution lies in a Nomadix Access Gateway that handles the visitor network access.

By definition, enterprise networks that provide Guest Access to visiting customers and partners are exposed to an ever-changing user base that is typically unknown by the network administrator. Without the Nomadix Service Engine™ (NSE) running on one our Access Gateways, giving access to visitors to the Internet may result in adjusting the PCs settings to match the LAN IP and proxy settings and raises a concern about unwanted attacks, which makes network security a concern for all users on the network and the network administrator.

Depending upon the size of the area and the number simultaneous guests expected, Nomadix provides the NSE on a complete family of Access Gateways. For larger deployments, the AG 5600 can be used. For mid-sized and small-sized deployments, the AG 3100 and AG2300 provide a cost effective platform and for single cell deployment.

This document presents an overview of a basic Guest Access network in an enterprise environment using a Nomadix Access Gateway while providing an overview of how that network is kept secure from un-trusted users and unwanted access; all this while removing the time-intensive task of configuring every guest's PC to match the settings of the enterprise network. The following sections provide details on how technologies such as Virtual LANs (VLANs) and Firewalls are used to ensure security when used in conjunction with a Nomadix Access Gateway.

Securing the Network

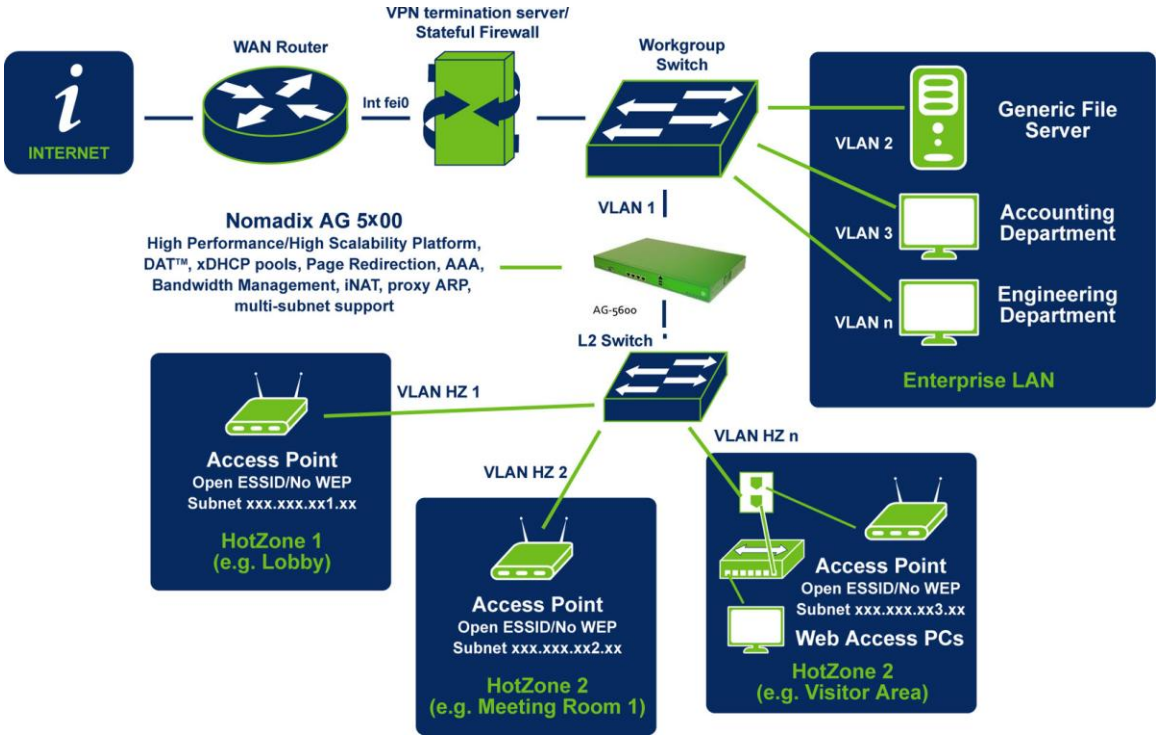
VLAN Security

A Virtual LAN (VLAN) is a logical network that can be created and secured from other logical networks on the same network LAN device, such as an Ethernet switch.

The NSE can track the location from which each user has requested network access by the user's unique VLAN identifier (ID). By using this method of user identification, the NSE can effectively manage secure access to the network.

Network Architecture

The following diagram shows an example of the Enterprise network architecture that might be deployed where VLANs are utilized to separate the traffic of the Enterprise's guests from the closed Enterprise network data, as well as showing how the use of a firewall will protect the network from an external attack (described in the following section).



The above diagram shows the Enterprise (secure private LAN) traffic is maintained on VLAN-2, 3 etc all branching off the main VLAN switch. A multitude of other VLANs are used to manage the Enterprise's guest traffic from a switch behind the AG 5600 with every VLAN ID representing a specific Visitor Area (Hot Zone). The specific VLAN designations are as follows:

- VLAN-2 is the (private) Enterprise Virtual LAN
- VLANs-3,n are for example used for specific departments offices in the closed Enterprise Local Area Network traffic
- VLAN-1 is used for the Visitor Network, i.e. the AG 5600 is located within this VLAN group.

Since VLANs separate the traffic logically, this configuration can provide security against an Enterprise Guest obtaining access to the closed Enterprise network.

Network Security and Plug-n-Play Access

Deploying a firewall in a network enables the network to be kept secure from unknown and unwanted users. The firewall can consist of a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to provide users with secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure. For example, it is usually desirable for the accounting servers and network to be kept secluded from the rest of the enterprise network, ensuring all unauthorized is locked.

Following are some of the techniques used to provide Firewall protection.

Packet Filter

Blocks traffic based on a specific Web address (IP address) or type of application (e-mail, FTP, Web browser, etc.), which is specified by port number. This can also be known as a "screening router."

Network Address Translation (NAT)

Network Address Translation (NAT), an IETF standard that allows an organization to present itself to the Internet with one address which is translated to many IP addresses internally, typically one per client computer. NAT also serves as a firewall by keeping the users individual IP addresses hidden from other networks by using private IP addresses that are not known to the outside world.

The NSE contains Nomadix' patented Dynamic Address Translation™ (DAT) technology to keep internal network users secure from an external attack. DAT also enables the Guest to get connected to the network without changing any configuration setting in their computer. The NSE also contains a URL Filtering feature that provides an additional level of security that defines which Web sites the network's users cannot gain access to, enabling up to 300 URL's to be blocked.

DAT was designed to eliminate IP configuration issues and their associated technical support calls and site visits allowing IT Administrators to deploy Guest Access without wasting valuable IT time and resources in providing this service to their partners and customers. Simply put, with Nomadix DAT technology in the network, Guest users can run their computers in any configuration and still gain access to the network. This is a vast improvement over standard networks where every computer must be assigned several specific settings to enable user access the network. As DAT performs translation much like 'basic' NAT it provides the same level of user security.

Typically, without DAT the following settings must be configured:

- **IP Address** — Unique identifier that allows traffic to be routed to the computer.
- **Subnet Mask** — Parameter that defines the size of the network segment on which the computer resides.

- **Gateway Address** — The network location of the gateway (router) connected to the Internet.
- **DNS Servers** — Addresses that specify the location of Domain Name Servers for the computer and translates these addresses, such as www.yahoo.com—entered by users into their browser, into an IP address such as 216.24.105.223 that computers use.

In a non-Nomadix enabled network, every one of the above settings must be correct in order for a Guest's computer to gain access. For example, if a laptop computer that is statically configured for an office location is moved to a home network location, it will be unable to access the home connection because the network settings will be different between locations, forcing the user to maintain knowledge of these technical settings and change them whenever they move between locations.

Summary

In summary, Enterprise networks can provide secure Guest Access to visitors in an easy to use, transparent fashion that doesn't take up valuable IT time and resources. The network can be protected by the use of VLANs and their ability to logically separate traffic within that network. In addition the local guest network is protected from external attacks by the use of NAT and DAT provided by the NSE running on our Access Gateways.

Note: *This document is intended as a guideline for network security. A network administrator that is trained and experienced in network security should be consulted before attempting to design and operate a secure network.*