Strategies for Lawful Intercept

Thursday, January 05, 2012

White Paper 230-1029-001

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

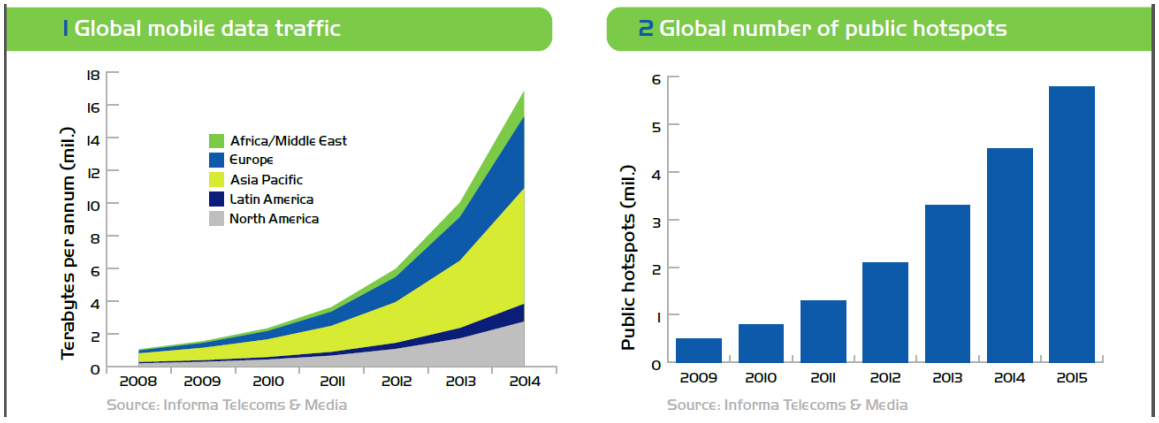
Contents

Introduction

Public access venues like guest networks, HotSpots and Digital Cites pose a unique security challenge to the industry. As the number of public access venues and the number of nomadic users continue to increase dramatically (see chart below), the requirement for new security mechanisms and the ability to aid law enforcement officials in their duty to protect society has become a paramount concern.

Nomadix' founders originally developed the core technology found today in the Nomadix Service Engine™ (NSE) Software for a government funded project, enabling nomadic users to access government applications. In the late 1990's, Nomadix was founded and the technology was put in commercial use to enable nomadic users to gain access at a variety of public access venues. These roots and Nomadix' continued desire to be conscientious "citizens" of the Internet led Nomadix forward in its quest to ever mature the Internet, protect its content and users, and continue to work toward making the Internet an invaluable tool for society.

Growth in Worldwide HotSpots (Number of Venues), 2008 - 2015



Security for network operators and subscribers to those networks has always been a key part of Nomadix' technology. Nomadix supports both user and network security features to address a variety of issues being faced in such networks.

Nomadix Gateways safeguard the user by employing features like its patented Dynamic Address Translation™ (DAT) and patented intelligent NAT (iNAT). These features translate the users' IP addresses thereby making it impossible to attack their computers from the Internet. Nomadix Gateways also support SSL login pages and VPN technologies that allow users to encrypt traffic.

In order to secure the network itself, Nomadix Gateways provide secure management interfaces and IPSec tunnels. They also provide network self-preservation and virus mitigation by

employing session rate limiting and automatic MAC address blocking. User access to the network is moderated by features like patented Home Page Redirection, support for RADIUS, Credit Card and Property Management Billing Systems that enable enforcement of a variety of authentication methods like UAM, Smart Clients and 802.1x

To address liability issues for Venue Owners and Public Access Service Operators (PASOs), all Nomadix Gateways support Terms of Use/Agreement pages that can be displayed to the Users. This forces the user to acknowledge the code of conduct they are expected to follow while using the network.

Though all the features stated above adequately address the security requirements of the users and the networks, they fall short of the unique requirements for lawful intercept (LI). The remainder of this paper outlines the Nomadix LI strategy.

Definition

Whatis.com defines Lawful Intercept as follows

''Lawful interception (LI) is the legally sanctioned official access to private communications, such as telephone calls or e-mail messages. In general, LI is a security process in which a network operator or service provider gives law enforcement officials access to the communications of private individuals or organizations. Countries around the world are drafting and enacting laws to regulate lawful interception procedures; standardization groups are creating LI technology specifications."

Requirement of LI in Public Access Networks

Most public access technologies rely on some kind of Network Address Translation (NAT) while providing access to visitors. This is done primarily to save public IP addresses, which tend to be expensive. NAT offers security to the end user by restricting access to the end user computer from the Internet and in the process offers anonymity to a public user. This anonymity presents challenges when Lawful Intercept is required.

There is a huge concern that public access networks will provide a safe-heaven for users who want to carry out illegal activities on the Internet. These activities include illegally downloading

copyrighted material from the Internet, sending threatening emails or engaging in illegal activities in chat rooms.

Additionally, venue owners who offer public access networks and utilize them as a marketing vehicle do not want to have their brand associated with any negative activity on the Internet or be exposed to the potential liabilities associated with not taking the appropriate measures to safeguard such activities.

Nomadix LI Strategy

Nomadix provides a range of public access Gateways that use the Nomadix Service Engine Software to provide seamless access to public users. Nomadix solutions enable any kind of user with varied client configurations to get onto the network without making any changes or adding client side software to their laptops or handheld devices. While our technologies simplify the process of getting access, we are acutely aware of the Lawful Intercept issues and requirements. Nomadix has a detailed set of solutions and strategies that enable Public Access Service Operators and Venue Owners to comply with Lawful Intercept requirements.

LI using Public Address Assignment

The NSE provides features that enable automatic provisioning and assignment of publicly routable IP addresses. With the IP-Upsell feature, all users accessing the public access network can be forced to have a public IP address. The traffic of such users does not undergo Network Address Translation and can be traced back to the original user. Additionally, the NSE can also be configured to turn its Dynamic Address Translation™ (DAT) feature OFF, allowing users with DHCP option enabled to access the network.

LI using Trace-Back Logs

The NSE provides tracking logs, which can be enabled to monitor all the port assignments for the users accessing a public network. These tracking logs enable you to trace-back to a particular MAC address and Username based on port and IP information available to an external site that has been attacked, hacked or used in an illegal fashion.

White Paper

The tracking logs carry the following information.

Purpose: How to interpret the Subscriber Tracking Syslog messages in version 2008.2.016. Subscriber Tracking messages are generated for misconfigured subscribers or those with proxy enabled in their browser. These syslogs are sent in CSV format so they can be imported into any application of your choosing. A message is generated each time a subscriber is added or removed from the Subscriber Database or the Current Subscribers table; for each session that the user generates; and if enabled, for every 500th packet incoming or outgoing for the subscriber.

1 2 3 4 5 6 7 8 9 10 11 12 13
conSTR,2008-06-10T22:33:05.20Z,00:50:DA:55:47:87,S(10.0.0.12:2307),P(10.10.10.10:8080),R(208.111.145.158:80), X(67.130.149.163:5156),TCP,Nomadix, Admin, joe, 10 ,10

1	Identification	the type of packet being reported
	subADD	the subscriber has been added to the subscriber database
	subDEL	the subscriber has been removed from the subscriber database
	subSTR	the subscriber has been added to the current subscribers table
	subEND	the subscriber has been removed from the current subscribers table
	conSTR	the subscriber session has been added to the DAT table
	conEND	the subscriber session has been removed from the DAT table
	pktSUB	the subscriber has sent 500 packets
	pktNET	the NSE has received the 500 packets for the subscriber
2	Time Stamp	UTC format as specified in RFC 3339
3	MAC address of the subscriber	
4	(S)ubscriber IP and Port	
5	(P)roxy IP and Port	
6	(R)emote IP and Port – the destination IP address for the session and the port used for the session	
7	(X) Translated IP and Port – the IP address and port used by the NSE for the session	
8	Protocol being used for session	
9	Site name as configured in the Configuration/Location/Site Name entry	
10	User access – the way that the user authenticated on the NSE	
	non-auth	AAA is disabled or the subscriber has not yet authenticated
	free	AAA is enabled and the subscriber has free access
	radius	AAA is enabled and the subscriber has logged in via Radius
	admin	AAA is enabled and the subscriber profile was created by an administrator
	CC user	AAA is enabled and the subscriber was added by credit card authentication
	PMS user	AAA is enabled and the subscriber was added by PMS authentication
	invalid	Closed session for a subscriber no longer on the NSE or is a Pending subscriber.
11	User name entered by the subscriber when authenticating	
12	Location from the Port Location table entry	
13	Port – the port the user is on. This could be either VLAN or SNMP Query for port identification	

If the information for the field is not available, then it will just have a comma for the field as in this example.
conSTR,2008-06-10T22:33:05.20Z,00:50:DA:55:47:87,S(10.0.0.12:2307),,X(67.130.149.163:5156),TCP,Nomadix,Admin,,,

A Sample Tracking Log example:

- Subscriber Added / Removed

subADD,2008-03-28T18:21:37.93Z,00:0A:E4:2F:BF:BA,,,,,,Newbury,Admin,UserOne,Room001,104
subDEL,2008-03-29T18:21:37.93Z,00:0A:E4:2F:BF:BA,,,,,,Newbury,Admin,UserOne,Room001,104

- Subscriber session Start / End event

subSTR,2008-04-30T20:32:43.50Z,00:10:A4:BA:BD:5C,,,,,Newbury,non-auth,,,
subEND,2008-04-30T20:33:28.70Z,00:10:A4:BA:BD:5C,,,,,Newbury,RADIUS,1024,,

- Start / End of a connection

conSTR,2008-03-28T18:21:37.93Z,00:0A:E4:2F:BF:BA,S(10.149.88.7:138),,
R(109.7.25.255:138),X(70.75.6.57:5001),TCP,Newbury,CC,UserOne,Room001,104
conEND,2008-03-29T18:21:37.93Z,00:0A:E4:2F:BF:BA,S(10.149.88.7:138),,
R(109.7.25.255:138),X(70.75.6.57:5001),TCP,Newbury,CC,UserOne,Room001,104

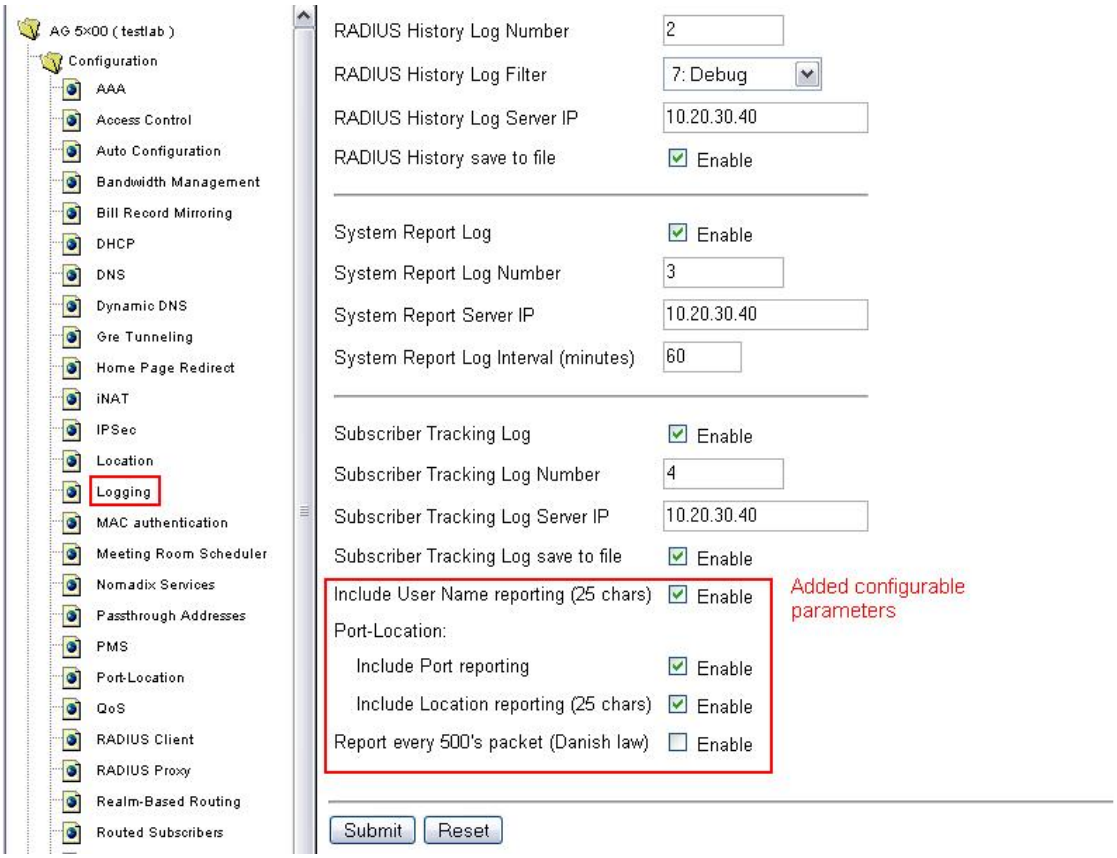
- Start / End of a connection with proxy usage

conSTR,2008-03-28T18:21:37.93Z,00:0A:E4:2F:BF:BA,S(10.149.88.7:138),P(109.7.25.10:80),
R(109.7.25.255:138),X(70.75.6.57:5001),TCP,Newbury,CC,UserOne,Room001,104
conEND,2008-03-29T18:21:37.93Z,00:0A:E4:2F:BF:BA,S(10.149.88.7:138),P(109.7.25.10:80),
R(109.7.25.255:138),X(70.75.6.57:5001),TCP,Newbury,CC,UserOne,Room001,104

- Packet Count triggered reporting

pktSUB,2008-03-28T18:21:37.93Z,00:0A:E4:2F:BF:BA,S(10.149.88.7:138),,
R(109.7.25.255:138),X(70.75.6.57:5001),TCP,Newbury,CC,UserOne,Room001,104
pktNET,2008-03-29T18:21:37.93Z,00:0A:E4:2F:BF:BA,S(10.149.88.7:138),,
R(109.7.25.255:138),X(70.75.6.57:5001),TCP,Newbury,CC,UserOne,Room001,104

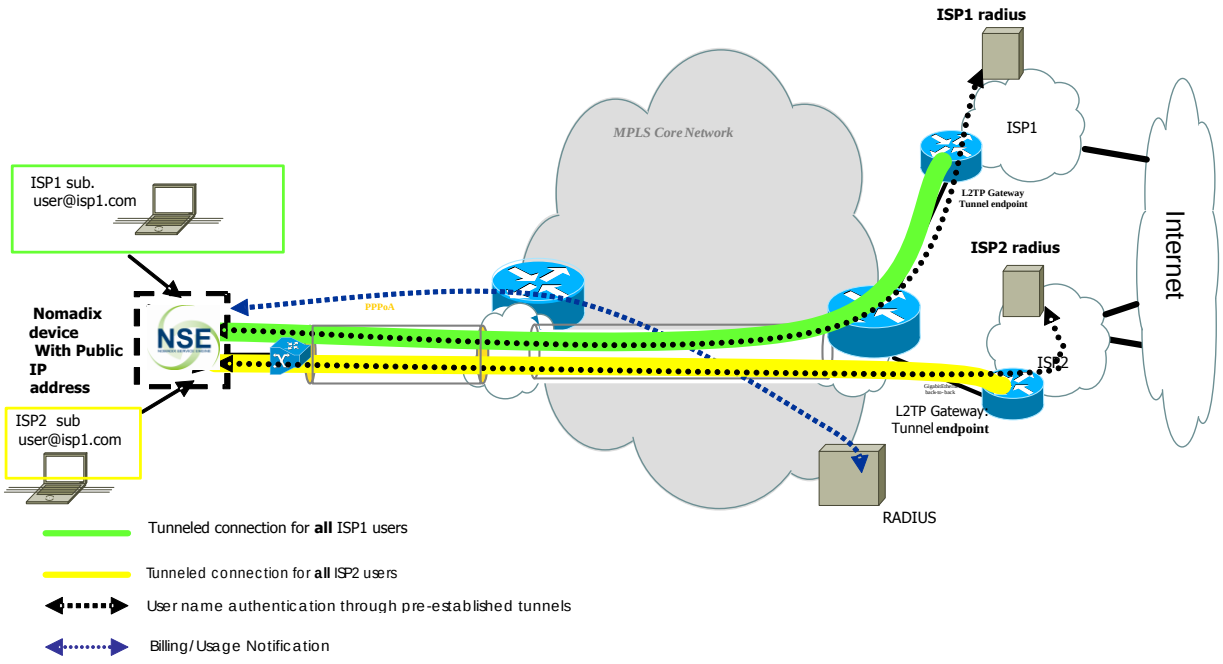
NSE: Lawful Intercept – Logging Configuration



LI using Tunneling

The L2TP Tunneling feature enables the Nomadix device to act as an L2TP Access Concentrator (LAC) and initiate single or multiple L2TP tunnels to different L2TP Network Servers (LNS). This capability can be used very effectively with the RADIUS Realm Routing feature to initiate tunnels based on the user Realm or Network Access Information (NAI). Realm specific traffic can be routed to a private network specific to that realm through these tunnels.

L2TP tunneling requires authentication with the 'home' RADIUS server and since all the subscriber traffic is tunneled to the ISPs 'home network', all the traffic can be monitored for Lawful Intercept purposes.



L2TP Tunneling

LI using Standard Protocol

There are numerous Lawful Intercept standards and numerous Lawful Intercept Forums. A short list of these can be accessed on the Global LI Industry Forum site at:
http://www.gliif.org/standards_activities.htm

LI is a sensitive issue since it involves issues pertaining to privacy rights. There is a debate on whether LI strategies help protect privacy rights by enabling methods to isolate and precisely target specific users or whether these strategies provide a tool to invade on privacy rights. As this debate continues, PASOs and Venue Owners are faced with providing solutions dictated by current, local legislation.

There are quite a few "standards" in place today and Nomadix feels that there isn't a commonly accepted or widely used standard. Nomadix continues to track these standards bodies and will work with the industry to incorporate widely accepted standards and practices applicable to a public access Gateway.

Conclusion

As Internet usage and the introduction of new applications like VoIP in a public access environment continues to increase, Service Providers will be required to provide more tools to aid law enforcement officials in tracking criminal activity over the Internet. Public access Gateways play a critical role on connecting nomadic users to public access networks, and are the ideal place to start the process of tracking illegal activity.

Lawful Intercept is important and Nomadix already has several features in place to aid PASOs and Venue Owners in supporting LI requirements. Nomadix is committed to tracking this part of the industry and providing new LI features as standards solidify and market requirements dictate additional techniques approaches.