User Personalized Networks – Pushing Security Closer to the User

William Osterman

December 26, 2001
Assignment Version 1.2f
Administrivia Version 2.0

Abstract

This paper discusses an emerging technology that allows an IT staff to implement a solution which provides for authentication, and service level authorization using intelligent edge-devices (switches) at the user point of entry. Technologies which support this solution, such as 802.1X are briefly touched upon and the architecture and benefits of the solution are described.

Introduction

Networks, in and of themselves, are complex and ever changing. Combine this with the fact that "connectivity" is becoming increasingly more important and widespread for businesses that want to compete in the marketplace – and someone's life has just become difficult. Just keeping the network up and running is a difficult and time consuming job, and not to mention, critical to business.

In the computer sense, a network is two or more devices connected together. Networks are used for many things including, but not limited to, sharing resources and collaborating on work. The very nature of networks is a double edged sword. While providing a medium for exchange, it provides an avenue to compromise "others." It is a threat to privacy, and consequently, to security! It is part and parcel to business and to life as we know it.

Network security is a simple idea, but a complex subject. It involves, in the simplest terms – determining what is at risk and then, attempting to protect it. As stated earlier, the very concept of a network is a threat to security. Danger can come from almost anywhere. The larger a network – the more connections, the more resources, the greater the danger. There is no getting around this.

Network security can be generalized into categories. Some of these categories are listed here.

- Authentication schemes
- Authorization
- Anti-Virus Systems
- Perimeter Defense
- Network Architecture/Access Control
- Intrusion Detection

These features can be applied in various ways and at various points. A comprehensive security program should include the ability to authenticate and authorize users.

IT staffs around the world are implementing many technologies to protect themselves. Each of these things applies itself to one or more of the categories mentioned above. Firewalls and filtering routers are used to handle connections at the perimeter of a network. Access lists are used to restrict traffic to and/or from various entities at specific points. Anti-virus software is used to insure that known malicious code is not spread via the network. Intrusion detection systems are used to monitor the network and specific hosts for signs of "irregular" activities. RADIUS servers handle authentication requests. It is commonly accepted in the security world that not any one of these measures, or any others, will individually be proof against all threats.

User Personalized Networks hereafter referred to as UPN, applies itself to the first two of the three AAA's listed below while taking advantage of the network infrastructure.

- Authentication
- Authorization
- Accounting

Authentication and authorization are handled at the user point of entry into the network – a service enabled edge switch. This is an important aspect of UPN. To borrow a saying from another industry – Location! Location! Location! Where does the threat come from? How do I protect from that threat? The answer to these questions will determine which methods one will use to protect themselves. The truth is that many attacks originate from within an organization. UPN goes a long way towards securing the network from internal attacks by allowing for authentication and authorization at the point where a user and/or device connects to the network. The importance of this can not be overstated. It limits what type of traffic can traverse the network by creating an "intelligent" perimeter which can adapt to the needs and security requirements of the particular user in question. This is a powerful tool by itself. When combined with other security measures it will make a significant impact on the security stance of an organization.

The Problem

The big question: How do I, as an administrator, effectively handle traffic originating from within my network to protect those resources deemed necessary by the business practice and the IT staff?

Normally, providing access to network resources in a corporate enterprise usually means giving the user a desktop computer, which is in turn plugged into a network port, and a username and password. A normal user boots up their machine, logs onto the network and uses the appropriate resources. A great problem exists as a result. *While the NOS logon procedure does provide for username password authentication when accessing specific devices using specific protocols, it does nothing to control the traffic passing through the network in the first place.* There are a significant amount of vulnerabilities which may be exploited by someone – or from a controlled computer – ***without*** "logging on" to the network. Merely having access to the network port would allow for controlling other people's machines, stealing information, initiating scans, spreading viruses, disrupting service, and much more. There is also the possibility that someone – perhaps not even an employee – may plug into somebody else's user port and go from there.

The point is, that *"logging on" to the network is just as much a convenience as a security measure*. The amount and type of things which can be done without "logging on" is frightening.

Securing systems internally is a difficult and time consuming job and for these reasons numerous vulnerabilities exist. Many industry resources report that internal attacks are responsible for a significant percentage of attacks.

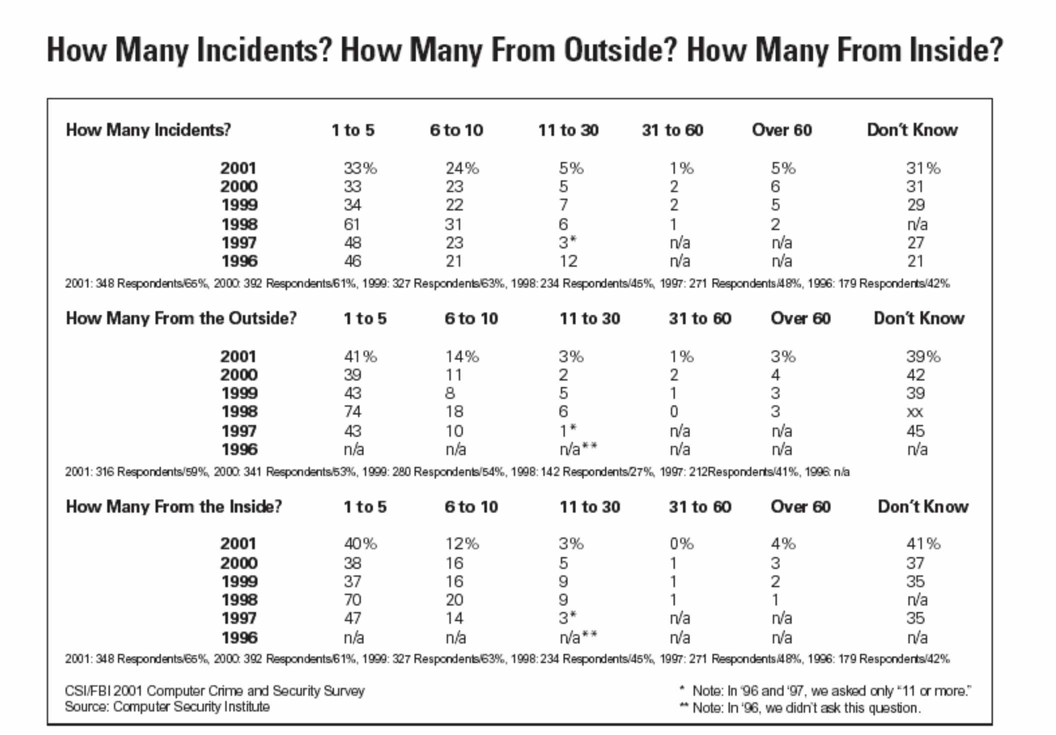
In 1998, the Computer Security Institute in combination with the FBI reports…

> …44% [of those surveyed] reported unauthorized access by employees…The most serious financial losses occurred through unauthorized access by insiders [Computer Security Institute. *Annual Cost of Computer Crime Rise Alarmingly Organizations Report $136 Million in losses*. Page 1. Spring 1998.].

In 2001 the trend continues. The Computer Security Institute in combination with the FBI reports that there is an increase in attacks from outside the network, but 31% of attacks were still internal…

> For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%) [Computer Security Institute, *Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar.* Page 4. March 2001].

The table below is taken from the CSI/FBI 2001 Computer Crime and Security Survey. The document deals with security and security trends. To get the document, go to http://www.gocsi.com/prelea/000321.html and fill out the request form. While both the quotes and the table do indicate that there is an increasing threat from external sources, they still indicate that a great many attacks come from the inside.



How Many Incidents? How Many From Outside? How Many From Inside?

How Many Incidents?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2001	33%	24%	5%	1%	5%	31%
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29
1998	61	31	6	1	2	n/a
1997	48	23	3*	n/a	n/a	27
1996	46	21	12	n/a	n/a	21

2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%, 1998: 234 Respondents/45%, 1997: 271 Respondents/48%, 1996: 179 Respondents/42%

How Many From the Outside?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2001	41%	14%	3%	1%	3%	39%
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39
1998	74	18	6	0	3	xx
1997	43	10	1*	n/a	n/a	45
1996	n/a	n/a	n/a**	n/a	n/a	n/a

2001: 316 Respondents/59%, 2000: 341 Respondents/53%, 1999: 280 Respondents/54%, 1998: 142 Respondents/27%, 1997: 212Respondents/41%, 1996: n/a

How Many From the Inside?	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2001	40%	12%	3%	0%	4%	41%
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35
1998	70	20	9	1	1	n/a
1997	47	14	3*	n/a	n/a	35
1996	n/a	n/a	n/a**	n/a	n/a	n/a

2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%, 1998: 234 Respondents/45%, 1997: 271 Respondents/48%, 1996: 179 Respondents/42%

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

* Note: In '96 and '97, we asked only "11 or more."
** Note: In '96, we didn't ask this question.

Add to this, the fact that is easier and easier to implement products and services on the network. Unfortunately, the ability to manage these resources in a secure way is not growing as quickly. This is indicative of most environments today. A study done by the Software Institute at Carnegie Mellon University has this to say.

> Engineering for ease of use is not being matched by engineering for ease of secure administration…..Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers…..Unfortunately, it is difficult to configure and operate many of these products securely. The gap between the knowledge needed to operate a system and that needed to keep it secure leads to increasing numbers of vulnerable systems [McDowell, Mindi (CERT/CC). *Who's Securing Networked Systems?* 2001]

The overall risk factors relative to network security are increasing for many reasons. More and more vital company information is stored and accessed via these networks. Jeffrey Lukowsky, a PhD on security, wrote an article entitled "Security Without Stress." The article deals with methodology similar to the UPN concept. In his article he makes some key points regarding risk and security methodologies – past, present, and seemingly future. Below is a comment which speaks directly to the problem.

> Most of this [risk exposure] can be attributed to the fragmented, "point product" approach to security implementation as wells as the lack of cost-effective management tools that can manage an entire infrastructure as a logical whole. Such management tools would need to include a simple powerful security engine in addition to configuration, topology, policy, monitoring, event correlation and other related tools [Lukowsky, Jeffrey (PhD). *Security Without Stress.* 2001].

The pattern is clear. It has been shown that a significant number of attacks are performed internally. The current methods are not adequate to protect internal resources from other users/devices on the internal network. Considering this, the appeal of the UPN solution becomes more apparent.

The Solution

UPN is one solution. It positions itself as a tool, which provides for simplified central management. It is not "point" specific, but amorphous and system wide. The perimeter moves from device to device, and port to port, with authentication and authorization at every desired point. UPN makes it simple to apply company "policy" at every necessary port within the enterprise easily and efficiently.

UPN is a solution that allows for access to the network for the services which are needed – and only for those services – by limiting the type of traffic (authorization) dependent upon who it is attempting to access the network (authentication). Just as importantly, it provides these mechanisms at the point of entry to the network. It does this while providing centralized administration through the use of roles and policy servers. These concepts and the mechanisms will be described in more detail later in this document.

The UPN solution allows for authorization of traffic based upon classification of information contained in the packet headers. Various network protocols like SNMP, telnet, NetBIOS, DLC, IPX, and others can be grouped accordingly. Additionally packet handling services, such as quality of service (QoS), class of service (CoS), VLAN assignment, and others can be applied.

Note: The classification and authorization services are not limited to the IP protocol suite, but include IPX, DLC, SNA, and others. Further information will be provided in a later section.

Currently there is only one vendor, Enterasys Networks©, capable of delivering this solution.

As stated earlier, UPN relies on authentication and authorization at specific points of entry into the network. ***Authentication*** is the process of proving one's identity. ***Authorization*** is the process of deciding what privileges accrue to the authenticated identity [Bellovin and Cheswick, *Firewalls and Internet Security: Repelling the Wily Hacker.* Page 119].

The draft standard for Port Based Network Access Control IEEE Std 802.1X-2001 demonstrates the first step on the road to this solution. It speaks to authenticating users at the port of entry and the mechanism involved. In its abstract, the standard states:

> *Abstract: Port-based network access control makes use of the physical access characteristics of IEEE 802, Local Area Networks (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails* [IEEE std 802.1X-2001. *Port Based Network Access Control.* Page 1. March 2001].

In summary, the IEEE standard defines a method for authenticating users connecting to edge switches and authorizing whether or not traffic may pass. The standard speaks in very simple terms. It deals with the following question and in the manner stated. Is one authenticated, yes or no? If not, the user has access only to authentication services. If yes, one is authorized for full access to said port and all services connected via this port. This concept is stated in more technical terms in the standard.

> *Access control is achieved by the System enforcing authentication of Supplicants that attach to the System's controlled Ports (see 6.3); from the result of the authentication process, the System can determine whether or not the Supplicant is authorized to access its services on that controlled Port. If the Supplicant is not authorized for access, the System sets the controlled Port state to unauthorized. In the unauthorized state, the use of the controlled Port is restricted in accordance with the value of the OperControlledDirections parameter associated with that controlled Port (6.4), preventing unauthorized data transfer between the Supplicant and the services offered by the System* [IEEE 802.1X-2001. *Port Based Network Access Control.* Page 30. March 2001].

Please note that the *Supplicant* mentioned in the above paragraph refers to the user attempting to access the controlled port. The *System* refers to the edge device. Additionally, the "*OperControlledDirections"* parameter referred to above is indicatory of the direction of the traffic being authorized and has two options – bidirectional or inbound (from the point of view of the edge device).

Essentially, the 802.1X standard deals only with the authentication mechanism relating to communications between the user and the edge switch. It does not discuss in any detail how the edge device, the switch, will authenticate the user. Nor does it provide any options for authorizing particular services (applications). It is all or nothing. These limitations would hinder implementation in the real world.

Note: Currently the 802.1X standard has not been ratified. Additionally, there are not 802.1X clients for most of the operating systems in mainstream use.

UPN brings the following additional components in to play.

- Authentication mechanism
- Centralized role based administration
- Service level enabled switches

Each of these items will be dealt with in more detail in the next section.

Implementation

The UPN solution is modular in design and can therefore support different configurations. Currently, Enterasys Networks© service enabled hardware must be used and these devices currently support 802.1X and web-based authentication in combination with RADIUS services. Most RADIUS servers though, can forward authentication information onto various sources, including various Network Operating Systems (NOS), RSA SecurID©, and others. The further authentication used by the RADIUS server in question is not critical to the UPN solution. Any authentication mechanism supported by the RADIUS server may be used to authenticate a user via the UPN solution. Any examples used in this document will pertain to the Windows© Network Operating System (NOS) and the Steel Belted© RADIUS server.

Each of the three components, and their associated requirements, mentioned in the previous section will be dealt with individually. The particulars for the specific configuration of each device are outside the scope of this document; therefore, they will be omitted. The items discussed below will be viewed at a higher level.

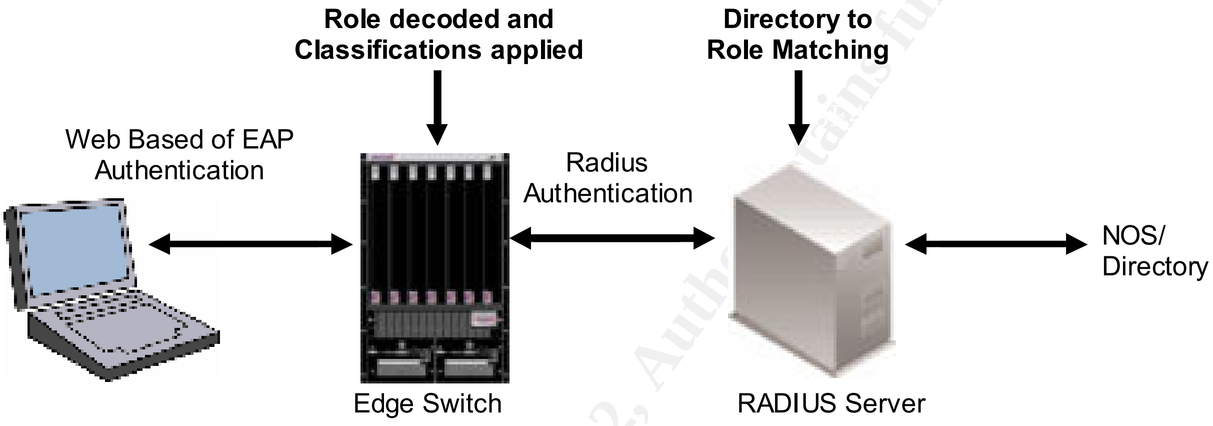
Authentication

The authentication mechanism has discrete communication steps and involves the user, the edge switches, the RADIUS server, and in our case, a Windows© Domain.

1. The user communicates with the edge switch and exchanges a username/password combination. Currently, web-based authentication and EAP from the 802.1X standard are supported, although there are not many 802.1X clients currently in use in the marketplace.
2. The edge switch proxies the username and password and passes it to a RADIUS server.
3. The RADIUS server in turn passes the username/password combination to the Windows© Domain.
4. The Windows© Domain returns an authentication passed or failed.
5. The RADIUS server takes this value, and adds a preconfigured filter id to the authentication packet, if authentication is successful, and is then forwarded back to the edge switch.

6. The edge switch then replies to the user and begins to enforce (authorize) the services appropriate to the role the port is now playing as a result of the authentication process. The filter id sent by the RADIUS server is used to identify the user role previously configured on the switch through the policy manager.

Below is a diagram taken from an Enterasys Networks document outlining the UPN process [Enterasys Networks. Available at http://www.enterasys.com/upn/#model] It displays the authentication process on a device by device basis showing the order of interaction.


Role decoded and Classifications applied
Directory to Role Matching
Web Based of EAP Authentication
Radius Authentication
NOS/ Directory
Edge Switch
RADIUS Server

© 2001 Enterasys Networks

An important factor in the above steps which might have been overlooked is worth mentioning again. The IT staff gets to leverage the existing authentication mechanism and information pertaining to the user base by authenticating (in the end) with the existing Network Operating System (NOS). There is an alignment of identities that should be adhered to as one moves through the authentication process – assuming an authentication success. A "role/filter id" defined on an edge switch is analogous to "filter id/user/group" on the RADIUS server is analogous to a "user/group" in the existing Windows© Domain.

For those of us who are a little more skeptical, one may view this in a slightly different manner. Building the roles for the edge switches will provide valuable feedback for those configuring your NOS as the underlying services being provided to users in any given configuration are better understood. This procedure, applied correctly, will allow the IT staff to more specifically define access to the network based on the necessary requirements at all levels (ie., group associations, types of network traffic, when and where to authenticate, etc.).

> **Note:** It is important to realize that even though one is leveraging the existing NOS for authentication information. The mechanism here is in no way a replacement for a user having the proper privileges somewhere else in the network and does not change the fact that any other existing authentications will have to be successfully performed. In fact, it is necessary that the different mechanisms play well together. A failure at any point will mean lack of access – whether good or bad!

Centralized Role Based Administration

The administration of the UPN solution revolves around the Enterasys Networks NetSight© Policy Manager. This is where the work of role configuration is done. The system requirements for this system are listed in the appendix at the end of this document.

Let us look a little more closely at what a ***role*** is in the UPN solution. A role is a way of identifying a group of services which may or may not be allowed through a port. Furthermore, handling parameters such as QoS, VLAN assignment, and others may be applied to the authorized traffic. The suggested methodology aligns business function to service to role. This alignment should allow administrators to easily implement the technical aspects of business needs.

> **Note:** The role that a port is enforcing does not in any way affect the privileges that a user will need in order to access various systems on the network. It merely defines the types of application traffic which may traverse the port in question. It is therefore, part of an overall security solution.

The NetSight© Policy Manager allows for the easy creation of roles, which are in turn configured on the edge devices at will by the policy manager. A change may be applied individually and/or by groups to all enabled switches and/or particular ports on a switch. Roles can also be imported and or exported. The policy manager does not have to be online for normal operation to occur. It is only necessary for applying changes.

In summary of the policy side:

1. A ***role*** is created.
2. ***Services*** are associated with the role.
3. An ***id*** is associated with the role.
4. The role is ***pushed*** to the edge devices and the specific ports in question.

One may use the pre-existing services and/or create ones at need. The process is relatively simple.

Service Level Enabled Switches

The edge devices rely on the policies created at the policy manager, and the proper authentication mechanism, but they are the ones actually doing the work of inspecting the traffic and dealing with it appropriately. They also proxy the authentication request from the client and pass it onto a RADIUS server. The switches are the work horses of the UPN model. The bulk of the work that the switches do is related to the classification of data packets. Classification is the ability to differentiate data based upon various characteristics.

The currently available methods of classification are:

- Port-based

- MAC address
- Protocol
- Layer 3 protocol type and type of service
- Layer 3 address
- Layer 4 socket/port

The benefits of classification are as follows:

- Containment of frames within specific boundaries (VLAN)
- Filtering unwanted protocols, applications, and users from the network.
- Securing specific resources, such as IP addresses.
- Packet handling parameters like QoS and CoS.

The switches are layer 2, 3, and 4 aware with respect to the OSI model. They are capable of discriminating data on the areas mentioned above. This ability, for instance, would allow one to filter out all traffic except DHCP, DNS, HTTP, and HTTPS for particular users [Enterasys Networks. Available at http://www.enterasys.com/products/whitepapers/switching/layer-primer/].

The switches are also capable of modifying the behavior of the data. Some of the parameters that these service level enabled switches work with are; Quality of Service levels (QoS), Class of Service levels (CoS), and VLAN assignment. In the end, any "service" that the switch is capable of performing can be used in configuring "roles."

AN EXAMPLE

The UPN solution fits very well into places such as universities and enterprise environments. In order to better understand the potential, let us describe a sample scenario. Let us assume we are on a campus environment. We would like to have three levels of service – student/guest, teacher, and the network administrator – available at each user port.

For the student/guest role, we would provide the following abilities:

- This might include DHCP (68/udp) to obtain an IP address
- DNS for name resolution (53/udp)
- HTTP (80/tcp) and HTTPS (443/tcp) for internet browsing
- SMTP (25/tcp) for email
- and ICMP (protocol 1) for network messaging

This will be defined as the default role for the port, indicating that these services would be available to users who did not authenticate or whom failed authentication.

For the instructor role, which is a "trusted" individual, we would provide the services mentioned for the student/guest. In addition, we would provide the ability to

- Connect to the Windows© Domain and its various resources such as file servers (NetBIOS)

This would require a successful authentication as an "instructor"

The network administrator role, the most "trusted" role, would give access to all services via the port in question. This would require a successful authentication as a "network administrator".

Implementation of this scenario is not trivial, but does not require great resources either. One, the service level enabled edge switches need to be configured to communicate on the network. This entails the proper IP and RADIUS server parameters. Most of this work is done anyway for proper monitoring of the network environment. Two, the RADIUS server needs to be configured to communicate with both the switches and the Windows Domain. No extra configuration needs be done at the Domain level as one is taking advantage of the existing domain infrastructure. Third, configure the policy server with the three roles and assign the appropriate resources discussed above. Push the policies to the desired switches and switch ports. Lastly, the switch needs to be configured to be aware of incoming client authentication requests. Done!

The process at work:

1. Policies are created at the Policy Manager and "pushed" to the edge devices.
2. The user logs on and authenticates through the edge switch, the Radius server, and finally with the NOS (i.e., Windows NT Domain).
3. The NOS/Directory sends the authorization packet back through the RADIUS server. At the RADIUS server, the NT Domain controller or other grouping is matched to the appropriate policy profile through the use of filter IDs, which will in turn identify the "role" to be played by the user (student/guest, teacher, network administrator).
4. The switch receives the authentication frame and does two things. It checks to see if the user has successfully authenticated. It checks the filter ID to see if there is a role identified.
5. If the user has not successfully authenticated, the port remains in the default setting. If the user has successfully authenticated, the port is changed to the open state, and the defined role, with its appropriate classifications, is applied to that interface. Note: If the port state, or the authentication state changes, the port is set back to the default role.

SUMMARY

In short, UPN provides a centrally managed method for securing the type of network traffic at the point of entry into the network through the use of role based administration. UPN uses authentication and authorization and applies them advantageously at the point of entry into the network. UPN provides the ability to limit on a port by port basis – the protocol, the IP addresses, the application, and more. It is easily implemented and easily managed.

UPN is ideally suited for handling internal network security for corporate enterprises, universities, and other similar environments. Additionally, it has applications pertaining to any device which is internal, regardless if the attack originates internally or externally.

References

Bellovin, Steven M. and Cheswick, William R. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading: Addison Wesley, 1994. Page 119.

Computer Security Institute. *Annual Cost of Computer Crime Rise Alarmingly Organizations Report $136 Million in Losses*. Spring 1998. URL: http://www.gocsi.com/prelea11.htm. Page 1.

Computer Security Institute, *Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar*. March 2001. URL: http://www.gocsi.com/prelea/000321.html. Page 4.

Enterasys Networks. *User Personalized Network*. URL: http://www.enterasys.com/upn/.

Enterasys Networks. *Layer 2/3/4 Frame Classification Primer*. 2001. URL: http://www.enterasys.com/products/whitepapers/switching/layer-primer/.

IEEE Standard 802.1X-2001. *Port Based Network Access Control*. Tony Jeffrey, Editor. March 2001. URL: http://www.ieee802.org/1/pages/802.1x.html. Pages 1 and 30.

Lukowsky, Jeffrey (PhD). *Security Without Stress*. August 2001. URL: http://www.messageq.com/security/lukowsky_1.html.

McDowell, Mindi (CERT/CC). *Who's Securing Networked Systems?* 2001. URL: http://www.itaa.org/infosec/pubs/ISArticle.cfm?ID=7.

Steel Belted RADIUS. URL: http://www.funk.com/radius/default.asp.

Appendix

NetSight© Policy Manager System Requirements

Windows NT/98/2000

- Minimum P2-400 MHz, 128 MB RAM
- Recommended P3-550 MHz, 256 MB RAM
- Free Disk Space: 75 MB
- Swap Space: Twice RAM
- A CD-ROM drive (for hard-copy installation media)
- A mouse
- An SVGA color monitor
- Minimum Service Pack 5 for Windows NT
- An SVGA graphics card set to at least 16 colors and capable of supporting an 800*600 display
- A Network Interface Card capable of running NDIS or ODI network drives in conjunction with a TCP/IP stack

Solaris 2.6, 2.7, 2.8

- Minimum Ultra 5, 128 MB RAM
- Recommended Ultra 60, 256 MB RAM
- Free Disk Space: 150MB
- Swap Space: Twice RAM
- A CD-ROM drive (for hard-copy installation media)
- A mouse
- Recommended operating system patches