ENTERASYS USER PERSONALIZED NETWORK

Abstract

Successfully providing business-focused solutions mandates that vendors have an understanding of their clients overall business goals. As the globalization of connectivity continues to proliferate, the relationships between an organization, and its internal and external employees, partners, and customers is critical.

Successful solution providers must deliver real time solutions that are capable of understanding and reacting to these relationships. This allows corporate security policies to remain intact while expanding the capabilities of the IT system and the organization. The relationship between the individual user and the Services that enable them to effectively perform their job function must be understood and supported by the IT infrastructure. This paper describes Enterasys Networks' solution to this challenge: the User Personalized Network.

ENTERASYS NETWORKS™

Table of Contents

The User Personalized Network and the Business of Technology 2

Addressing the Challenges of the Current IT Business 3

Addressing the Challenges 5

- Authentication 5
- Role-based Administration 5
- Service-enabled Edge Infrastructure 7

System Walkthrough 8

- Policy Creation and Distribution 9
- User Authentication 11
- Authorization and Role Assignment 12
- Services Provisioning 13

Deployment of the User Personalized Network System 14

- Creation of the Relationship Hierarchy 14
- Enabling of Authentication in Shared Areas, and Specific Cases 14
- Wide Scale Deployment of Authentication and Dynamic Policy 15

Conclusion 15

"Success in the information economy will depend on a company's ability to use network technology to create business relationships."

—The Burton Group

The User Personalized Network and the Business of Technology

Today's IT systems are the lifeblood of an organization's ability to conduct business. This is a significant change from the not so distant past, in which the availability of the telephone, not the computer network, was the major requirement in conducting business. The fact that nearly all of an organization's business is now conducted over the IT infrastructure means that all of the information about that business is also stored within that IT system. Additionally, all users, regardless of business function, exist on the same IT system, presenting a significant challenge in terms of providing access to, and delivery of, information. In addition, non-business critical information, and traffic, also exists in that same IT network system. In most cases, this means that mission critical applications receive the same performance characteristics as someone planning a vacation over the Internet, or listening to Internet radio. This becomes even more troubling as the proliferation of interactive multimedia, Internet gaming, and peer-to-peer file sharing applications become prevalent.

These realities lead us to a conclusion that the security of stored data (files and records), and the delivery of interactive data (network traffic), must be managed if the IT system is to effectively serve the needs and goals of the business. In order to achieve this, the mode of thinking within the IT community must change. Technologies such as data encryption, filtering, permissions, Rate Limiting, VLANs, and QoS must be viewed as the facilitators or enablers of the solution, and not a solution in themselves.

While each of these mechanisms is critical in delivering a robust, secure IT system, they should be viewed as technological stepping-stones on the path to the ultimate solution. A discussion of what each user's experience with the network should be is a critical first step in deciding how to use these mechanisms. Additionally, in order to deliver an IT system that matches the needs of the business, an understanding of the human beings in the organization, and their relationship to the organization must be gained. It is only then that the appropriate technological solutions can be developed, and meaningfully deployed.

In the paper "*The Network Services Model: New Infrastructure for New Business Models,*" written by The Burton Group, the author states "Success in the information economy will depend on a company's ability to use network technology to create business relationships." This simple statement raises a huge question; How can network technology be used to create business relationships? Moreover: How to implement technological solutions, and realize the ultimate goal of people receiving the appropriate behavior? The answer is in finding the link between a person's use of the IT system, and the business results of those actions.

The first step in establishing that link is to gain an understanding of the concept of "Services." In this context, Services represents an abstraction that lies between the technological things a network user does, such as using protocols, consuming network bandwidth, or using applications, and the associated business functions that result from those technological actions, such as making sales or executing financial transactions. The introduction of the Services abstraction enables the separation of organizational goals from the technological details of how to implement them. To model this, Enterasys has created the Relationship Hierarchy, with Classification Rules at the base to define specific packet handling behaviors, Business Roles at the top to identify specific job functions in the organization, and Services in the middle, providing the glue between the two layers. Services actually form the backbone of the relationship hierarchy, the link between the business and the technology. These topics are described in detail later in this paper.

If the business paradigm and the IT capabilities can be modeled, the next challenge is to match an individual person to his/her place in the Relationship Hierarchy. This match requires that the network be able to react to the identity of the person. To date, the data network itself has not provided visibility into who the actual people in a network system are. There are certainly points within the IT system that understand the concept of people, typically the NOS, the Directory, and whatever other username and credential entities exist but the actual connectivity devices in the network have not, to date, understood the concept of people. There have been attempts in the past to build systems that deploy policy and security characteristics based on technological considerations such as MAC address, IP address or subnet, and even switch port location. Given the mobility of the workforce today, and the complexity of configuring such schemes, these mechanisms are clearly insufficient. The challenge, therefore, is to implement a system that understands who the person attempting to access the network is and apply the appropriate behavioral characteristics to that user based on their role within the organization.

Addressing the Challenges of Current IT Business

Now that the components of the solution has been identified, it's time to define the challenges that the User Personalized Network has been designed to resolve.

Historically, depending on the type and scope of the project, somewhere between 30-50% of all IT projects fail. One of the major factors attributed to the failure of IT projects is that the project's rationale or the goals were never well defined. Implementing a solution without clearly identifying the problem is a virtual guarantee for failure. To address these issues, the User Personalized Network has some high level challenges that it endeavors to solve. Because more specific goals should be set before implementation of a solution, the following should aid in building the framework of what problems will be addressed by this solution.

The User Personalized Network system is designed to address some of the most challenging problems facing IT departments, and the businesses they serve. They are:

- IT rules and goals are not aligned with Business rules and goals
- Complexity of the IT system must be minimized, while increasing its functionality
- Business must secure intellectual capital and the success of the business operations

The first challenge is likely to be the result of the speed with which the IT system became mission critical. The dependency of the success of an organization on technology has increased so rapidly that the two and five-year planning cycles have been shortened to six month, and one year planning cycles.

The time for research, analysis, case studies, and the like, has been virtually eliminated for two reasons:

- The first is that technology is changing so quickly that to invest extensively in research may result in the obsolescence of a proposed solution before it can be deployed.
- The second reason is that the people who can actually implement new technological solutions are not always focused on the needs of the organization.

These technology wizards are often motivated to implement technology for technology sake without considering the impact on the increasingly dependent business processes. Although there are certainly many other places to find blame for this phenomenon, the basic idea is that in order to keep up with the competition, the model became fund it first, see if it worked later.

What is occurring in today's market is that companies are accepting a few statements as true:.

- The first is that technology is critical to the success of their business, and is often the differentiator between them and their competitors.
- The second reason is that the shortage of IT talent continues to be a problem, but there is no shortage of new technological solutions, each potentially more complex than the last.

These solutions combine to mandate a business approach that says "We must keep up with our competition by deploying new technology, but this technology must be implemented with a clear impact on our business, and it must be manageable by the staffing levels we can maintain"

The second challenge to be addressed by the User Personalized Network was that the complexity of the IT system must be minimized, while increasing its functionality. There are innumerable technology bells and whistles that can be implemented in today's IT products. To date, vendors have not done a good job of providing methodologies for implementing complex technologies in an automated or simplified manner.

Furthermore, the realization is that implementing complex technologies can have two very dangerous side effects:

- First, if the implementation is too complex, the cost of doing so may outweigh the benefit to the business that the feature provided in the first place.
- The second, and equally important point, is that if the implementation of that technology is very complex, the troubleshooting and repair of that technology may be so complex that the benefit realized by implementing it is lost because of the inability to repair or adjust the system after implementation.

Any new solution therefore must provide three core capabilities: automation, simplification, and instrumentation. These combine to ensure that the dangers of implementing complex technologies are avoided.

"Industry hype notwithstanding, it is a fact that a demonstrable security infrastructure has become a business enabler in the e-business world."

—The Meta Group

The third challenge to be addressed in the User Personalized Network is that securing intellectual capital, and the success of the business operations, must be a priority. The Enterasys User Personalized Network solution provides the ability to have immediate, and identifiable, impact on the securing of intellectual capital as well as an impact on the successful execution of the business processes that run over the IT system.

Security of network stored data, in addition to the availability of data and business process over that network continues to increase in importance. In the report *"Selling Security: Obtaining Executive Support and Investment,"* the Meta Group states "Industry hype notwithstanding, it is a fact that a demonstrable security infrastructure has become a business enabler in the e-business world."

To date, the methodology for securing network data, and network resources has been one of a "discreet box" mentality. If security needs to be improved, add a firewall; if WAN links are oversubscribed, add a packet shaper; and if the network is prone to attack, add an Intruder Detection System (IDS). Although these technologies are important elements of a secure network system, there is a need to have the network infrastructure itself provide capabilities that have an identifiable impact on the security of the system. The User Personalized Network, positioned as the first line of defense against attacks at the closest possible point to the user, has the capability to create a more secure controlled environment

Addressing the Challenges

Enterasys is committed to identifying and addressing the needs and goals of today's IT department. As such, the User Personalized Network has been designed to provide a business-focused solution that will:

- Ease the IT administrative burden
- Provide secure, reliable connectivity to system users, based on who they are within that organization

The User Personalized Network is based on the reality that the only way to make technology truly meaningful to the business is to implement solutions that cater to the individual person's relationship to the business. In other words, instead of an IT system whose deliverables are QoS, Routing, Switching, and VPN, the deliverable for the IT system should be the user receiving the appropriate service levels to appropriately match his/her job function. Again, the technological considerations should be the mechanisms by which the goal is realized, not the goal itself. In order to deliver on these principles, three primary requirements must be present. They are:

- Authentication
- Role-based Administration
- Service-enabled Edge Infrastructure

Authentication

In order to understand who the people are in an organization, there must be a mechanism for discovering a person's identity. As mentioned, a person's identity is not represented by some of the mechanisms historically used in IT to assign policy information. For example, values such as the MAC address, IP address, or physical location within a network are not sufficient in determining the identity of a person. Presently, users can login on from different machines and negate the MAC address as well as the physical location as identifiers. Also, the proliferation of the Dynamic Host Configuration Protocol (DHCP) has made the IP host address powerless as an identifier. In fact, given the dynamic nature of IP address assignment, network managers should begin to view a user's IP address as an enabler of connectivity only, not as an indicator of the user's identity, and certainly not as the mechanism with which to enforce policy rules.

It quickly becomes apparent that the only consistent identifier for who a person is in a network system is their login, or their authentication credentials. This makes the concept of authentication the most viable option for discovering a person's identity. The problem, to date, has been that Local Area Network (LAN) infrastructure components have not participated in the authentication process. Instead, authentication has been viewed as a NOS, or security function, and not part of the network's responsibility. It is now obvious that the network infrastructure must participate in the authentication process if it is to assign the appropriate behavioral characteristics to the appropriate person. Enterasys is committed to delivering authentication as part of the User Personalized Network. As a result, a person's identity can now be discovered via authentication, at the point of ingress into the network system.

Role-based Administration

The idea that Services provide the glue between the business and the technology is an important concept in the functional delivery of the User Personalized Network. When configuring the system, the tools used must provide visibility into the business functions that exist, as well as the technological capabilities.

Every vendor in the networking space develops tools that configure, manage, or administer technological elements. In addition to configuring the technological capabilities, the vendor must have the ability to model the business in a way that non-technical people can understand. This allows both groups to have influence into the resultant behavioral characteristics of the user community.

Here again, the concept of Services becomes critical. Members of the IT staff will certainly understand the technical considerations of configuring the network system, while the business people will understand the nature of the organization. Services become the language that both groups understand as well as the common ground on which solutions that are meaningful to the organization can be created. In these discussions, there is no need for the business-focused members to understand the technologies that result in the delivery of an email. Nor is there a need for the technical individuals to understand the business models that result in one group of users receiving preferential delivery of their emails. The point is simply that through Services, both groups can have productive conversations about how IT can better serve the goals and needs of the business.

Role-based administration is the modeling of both IT and business considerations. This is achieved through the creation of the Enterasys Relationship Hierarchy, shown in Figure 1. In this graphic note that the business functions are modeled at the top (Roles), and technological considerations are at the base (Packet Classification Rules), with the Services layer providing the bridge between these two. This model simplifies the deployment of business roles by pushing the packet processing details below the Services layer in the model. The high-level focus can be on the specification of the roles in the organization and on mapping the appropriate Services to them. The details of the Classification Rules needed to realize each service can be left to technicians familiar with packet formats, frame types and protocols.

The ability to include Services in multiple Roles further simplifies the operation by eliminating the need to duplicate Service creation for each discreet Role. A Service can be constructed once, and used again as needed for as many Roles as is necessary.

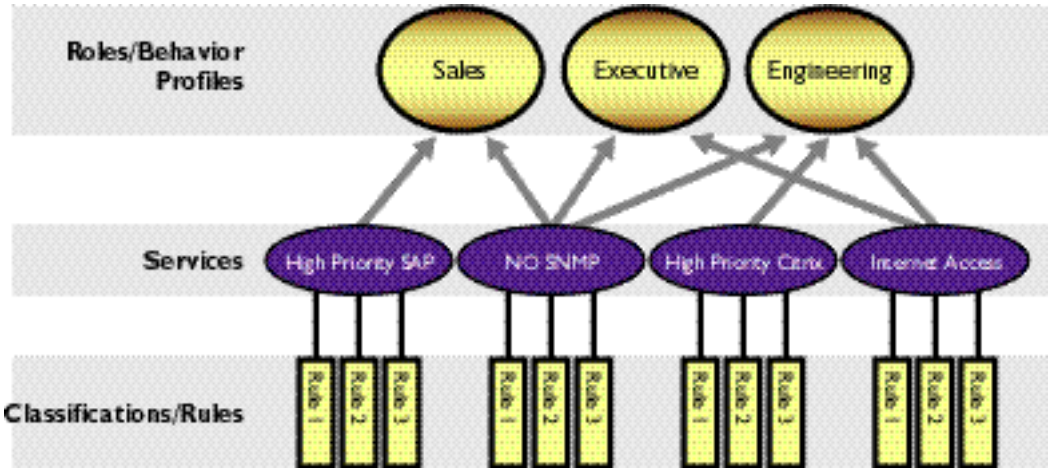

Figure 1: Enterasys Relationship Hierarchy

"The companies that have superior network infrastructure will have a distinct competitive advantage in creating e-business relationships. And the companies that fail to achieve that goal could well find themselves following instead of leading in their key markets."

—The Burton Group

Service-enabled Edge Infrastructure

The delivery of a Services-based network (one that can provide the appropriate Services to the appropriate person) requires an infrastructure that is highly flexible, and that can support very complex and granular rules at the service edge of the network.

Providing this kind of flexibility while maintaining the desired level of performance can only be achieved in a platform where the architecture was intended to deliver such Services.

The Burton Group states in the report *"The Network Services Model: New Infrastructure for New Business Models,"* that "The companies that have superior network infrastructure will have a distinct competitive advantage in creating e-business relationships. And the companies that fail to achieve that goal could well find themselves following instead of leading in their key markets." This statement highlights the importance of a network infrastructure that is capable of implementing very granular rule sets to provide greater security of both network stored data, and network bandwidth. Enterasys' edge products (including the Matrix E6 and Matrix E7) were designed and architected with this level of granularity. What is now facilitating the use of this functionality and making it even more appropriate for deployment in large networks is the automation and system-level control provided by Enterasys' innovative combination of authentication and policy-based management tools. Enterasys Matrix products have delivered the capability to provide very granular traffic control for many years, and have continuously made improvements in the granularity of rules sets, and the ease of configuration.

Delivery of the Service-enabled edge is achieved through the use of Classification Rules, implemented at the point of ingress for the user. These rules allow any number of actions to be implemented dynamically on any combination of Layer 2, 3, or 4 variables. A detailed description of Enterasys' classification capabilities can be found at http://www.enterasys.com/products/whitepapers/switching/layer-primer/index.html. It is most important to realize at this point that having the capability to deploy these rules does not fulfill the requirement. These rules must instrumented for deployment in an automated, system-level fashion, to achieve wide spread acceptance in large enterprise networks. System-level deployments require that the components that make up the network connectivity system be modeled as a single entity, or a small number of reasonably sized entities depending on the needs of a give scenario. This requires software that can understand the relationships, and dependencies between a number of network devices and configure them as a system. Additionally, automation is absolutely critical for the deployment of complex and granular rule sets. A model that mandates the management of complex rule sets on an individual, per element basis, would surely collapse under its own weight, either at implementation, administration, or troubleshooting.

Now that all three requirements have been outlined, the importance of each in delivering the User Personalized Network can be realized. The user cannot be assigned the appropriate behavioral characteristics without authentication. Behavior characteristics cannot be modeled, or delivered, without the appropriate software configuration and instrumentation tools. And the entire system will not deliver the desired result unless the network infrastructure was engineered to deliver the required capabilities. This unique combination of architecture and innovation is what allows Enterasys to deliver the User Personalized Network.

System Walkthrough

Having identified the challenges to be addressed, and the high level concepts that must be present in order to address those challenges, a system walkthrough is in order. For clarity, the system walkthrough will be presented in four major stages. They are:

- Policy creation and distribution
- User authentication
- Authorization and Role assignment
- Services Provisioning

Figure 2 provides a sample network design, which will be used to describe each of the four stages in the User Personalized Network. Notice, as each of the four stages is described, that there is a loose relationship between the components of the User Personalized Network system. That is, there is interaction between the authentication, authorization, the NetSight Policy Manager, and the Service-enabled edge products. However, note that there are no dependencies between the components of the system. This flexibility is critical for Enterasys, because it allows incremental enhancements and changes to occur within the User Personalized Network system, without requiring that the entire system be modified to support the changes. It also ensures against a loss of synchronization between the components of the system, a common occurrence in monolithic implementations. To be more specific, this modularity positions the User Personalized Network to support emerging protocols such as SNMPv3, COPS, Diameter, and any of the changes that are mandated by the AAA Authentication Authorization, and Accounting efforts currently taking place.

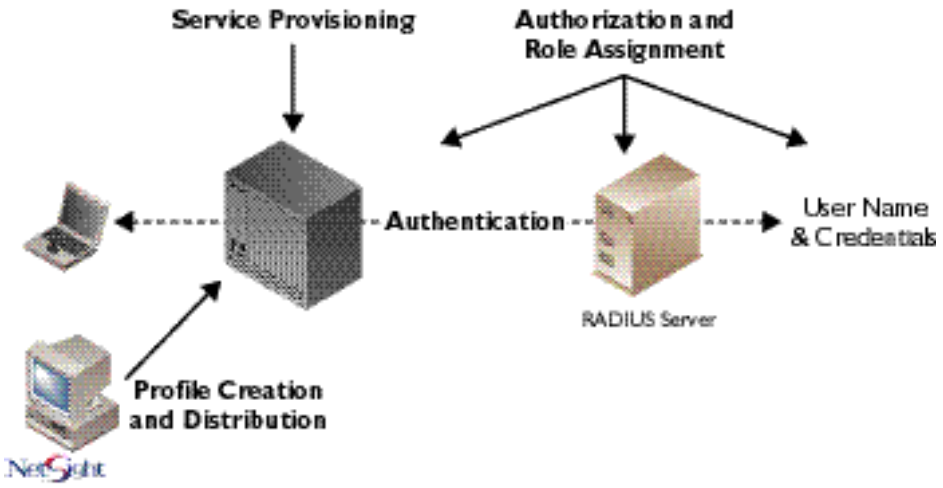

Figure 2: The User Personalized Network Solution

Policy Creation and Distribution

Enterasys' NetSight Policy Manager facilitates the creation and distribution of the Relationship Hierarchy. The process of creating the Relationship Hierarchy includes the configuration of the business Roles at the top of the hierarchy, the technological Classification Rules at the base, and the Services layer acting as the glue between the business Roles and Classification Rules. This hierarchy can be constructed manually, or it can be built using templates included with the Policy Manager software application.

The ability to import Roles, Services, and Classification Rules as well as topology information is an important feature of the NetSight application, as it facilitates a method to effortlessly add to the capabilities of Policy Manager. The ability to add support for emerging applications or changes in the business model, without changing firmware, hardware, or software is clearly an advantage for customers whose network requirements continue to grow and change. This ability stands in stark contrast to architectures in which the vendor is the only party capable of enhancing the Policy set, due to restrictions in the firmware, hardware, or software architectures.

In a typical scenario, the first tier of the hierarchy to be configured is that of the Roles (abstractions of the business functions that exist in an organization). Aligning the Roles with an existing organizational model is easily facilitated, and recommended, because there is no need to reinvent the structure of the organization. The time and effort that has already been invested in modeling the business can, and should be leveraged. Enterasys recommends but does not mandate, that the naming convention for the Roles be aligned with an existing structure within the organization. In many cases this would be the NT Domain or Netware Directory Server (NDS) naming conventions for groups of users. The potential importance of this action will become obvious in the sections that follow.

When configuring Roles, the network administrator also has the opportunity to configure some default parameters for that Role, prior to associating any Services. Examples of the default settings for a Role might include QoS, CoS, (including 802.1p, TOS, and Diffserv), and/or VLAN settings for all traffic from users in that Role. These basic settings provide an easy way to implement differentiated behavioral characteristics for groups of users, with very little configuration.

The development of Services is actually configured by creating combinations of Classification Rules that result in the desired network behavior. A Service can be as simple as assigning all email traffic to a certain priority, achieved by simple creating a Classification Rule that adds an 802.1p, ToS, or DiffServ value to all SMTP traffic. Services can also consist of a complex set of Classification Rules that include a combination of priority, filtering, rate limiting, and VLAN assignment. The complexity and granularity of the Classification Rules and Services is bound only by the requirements of a given situation or the imagination of those implementing the system.

Once this hierarchy is constructed, using a combination of business Roles, Services, and Classification Rules, it is distributed, (or "pushed") to the network system, shown in Figure 3. Once the network infrastructure has been empowered to enforce the Relationship Hierarchy, it does not require any further communication with the NetSight Policy Manager application.

Although the complete Relationship Hierarchy is always present on each network device in the UPN system, enabling a policy or Role on a specific network interface occurs in two ways: dynamically and statically. Dynamic policy will be covered in a separate section because it requires other elements of the system to be described prior to its description,. However, a discussion of Static policy, and its importance, is appropriate at this point.

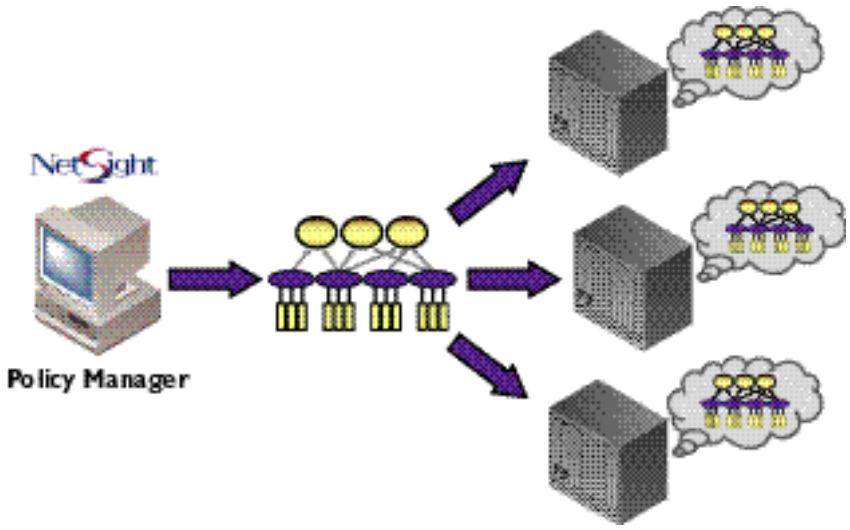

Figure 3: NetSight Policy Manager distributes the Relationship Hierarchy to the network edge, empowering the network to enforce the desired policy rules

The enforcement of the Relationship Hierarchy at the network interface level can be configured to occur statically on network ports for two important reasons:

- The first is that there are a number of devices within an IT system that do not require dynamic policy, or are incapable of authentication. These include printers, fax machines, and legacy devices such as software-based routers and shared hubs. NetSight Policy Manager provides the ability to configure default network behavior for ports that can benefit from static policy configuration. This is accomplished by configuring default Roles on the desired network ports and can be done using either pre-configured port groups, or by creating customized port groups to fit a given scenario. Examples of pre-configured port groups include all 10/100 ports, all backplane ports, or all Gigabit Ethernet ports. Examples of customized port groups are likely to include groups such as all printer ports, all server ports, or all proxy and firewall ports.
- Static policy can also be useful on authentication-enabled ports as well as those not configured for authentication. This will be discussed in the next section, which describes the authentication process within the User Personalized Network system.

User Authentication

Authentication is the key component to aligning the policy rule set with the individuals to whom that policy will be applied. Enterasys is providing two primary mechanisms for authenticating users:

- The first is the use of web-based authentication. Users who want to receive network Services access a secure web page (the web server actually resides on each switch) from a browser are asked to provide username and credentials. These credentials are then forwarded on to a RADIUS server, which either authenticates them, or forwards the request to the appropriate authenticator, such as an NT server, Active Directory, or NDS server. The key is that the Enterasys User Personalized Network is designed to utilize the existing security system and its username and credentials database, eliminating the need for implementers to install and configure a duplicated database for network-based authentication. This is a significant advantage when compared to approaches that utilize proprietary mechanisms to implement policy—or even to authenticate users as it leverages the work the customer has already done in implementing a security system for maintaining users login information. This interaction is also useful in assigning Role values to users, because the existing model in either NT domain, NDS, or Active Directory can be duplicated in the Relationship Hierarchy. This results in the recommendation that naming conventions for the Role values be aligned with the naming of an already existing hierarchy to aid in the configuration and troubleshooting of the system.
- In addition to web-based authentication, Enterasys is providing support for the 802.1X standard for authenticating users. This standard facilitates widespread and interoperable authentication in multi-vendor environments. Support for 802.1X is added in Microsoft's Whistler version of Windows 2000, and is likely to be supported in other Operating Systems, both windows and non-windows in the near term.

When deploying an Enterasys Authentication-enabled network, there are three primary port states that exist: *Authentication off / Port on, Authentication on / Port off,* and *Authentication on / Port on with default policy.*

- The *Authentication off / Port on* state is simply the network behaving the way it would in today's environment. Authentication is not required, and there may or may not be static policy rules applied.
- The *Authentication on / Port off* state occurs when users must authenticate to the interface prior to getting any kind of connectivity. It is the strictest of the port states, as the user can neither send nor receive any network traffic, except for authentication traffic, until he or she has successfully authenticated to the system.
- The third state, *Authentication on / Port on with default policy,* involves the enabling of authentication on the interface, but allows certain traffic to traverse that interface, either prior to authentication, or after a failed attempt to authenticate. In this scenario, it is likely that users would be allowed to use basic network Services, such as Internet, or NOS login, but not access other areas of the network, or consume large amounts of network bandwidth. Alternately, all of the ports that don't have authenticated users might restrict all of their traffic to a lower priority until they authenticate. This allows the network administrator to allow basic network connectivity to users that need it, such as consultants, or temporary employees but to not expose them to all of the organization's resources and available Services.

Finally, remember that it is the authentication process, the idea of discovering who the actual people are in a network system that is one of the three key components of the User Personalized Network. Authentication then, is a critical first step in assigning dynamic network policy to the "people" in an organization. Once an individual user has been identified the process of assigning the appropriate policy to them can begin. That is the topic of the next section.

Authorization and Role Assignment

Authorization and Role assignment occurs in two places: first in the existing username and credentials database, and secondly at the switch port to which each user is attached. Please refer again to Figure 2. In this figure, there are actually three points at which the Authorization and Role assignment is occurring. Remember that the RADIUS server can either authenticate the users itself, or proxy that responsibility to a separate username and credentials database. As a result, Figure 2 shows three lines, but in actuality, the RADIUS server and whatever other username and credentials database exists combine to deliver the authorization functionality, thus there are three arrows in the figure, but the two functional areas of authorization.

It is important to note, at this point, that Enterasys has not implemented any proprietary additions to the RADIUS system, allowing the use of many different RADIUS server products that are likely to already exist in the client's network. When the authentication information is received from the end station by the switch, it is forwarded to the RADIUS server. The RADIUS server, in turn, either authenticates that user, or forwards, (proxies) the authentication information of that user to another entity for authentication, typically an NT Domain, NDS, or Active Directory. If that authentication fails, the response back to the switch causes the port to either remain off, in the case of the *Authentication on / Port off* state, or to continue to provide default system behavior, in the case of the *Authentication on / Port on with default policy* port state.

If the authentication is successful, the RADIUS server appends a Filter ID field to the success message that is sent back to the switch. The Filter ID field is a text string that contains a Role name that can be used by the switch to understand how that specific user fits into the Relationship Hierarchy.

The RADIUS server knows the value to append to a given user during an authentication attempt because the RADIUS server has been configured to align users with the appropriate Roles. This can be done by aligning the existing organizational structure with that of the Roles in NetSight Policy Manager. A common example would be that of an NT Domain, where the names that exist in the domain are configured to match the Roles in NetSight Policy Manager with the same names from an NT domain or NDS group. Although this was mentioned in the Policy Creation and distribution section, the importance of selecting a well-known naming convention for the Roles in Policy Manager is worth stressing again.

Administering and troubleshooting the system is certainly much easier in a system where the policy rules match those of the other organizational structure that exist in the IT department. Alternatively, or for exceptions to the norm, users can be configured individually to exist in certain Roles, which also achieves the desired result. This type of configuration is more time consuming than aligning existing groups with the Roles in Policy Manager; it is recommended that this method be implemented conservatively.

The result of the Authorization process is that the user has now been matched with the appropriate Role within the organization based on their identity. The last stage is to implement the appropriate Classification Rules on that interface, ensuring that that user receives the desired service levels and behavioral characteristics.

Services Provisioning

The final stage in the User Personalized Network is the provisioning of Services or behavioral characteristics to the users that have successfully authenticated. As mentioned earlier, the ability to configure Default Role settings in a network system allows certain Roles and Services to be provisioned by default. The process for doing this is simply creating the desired Roles, Services, and Rules in NetSight Policy Manager, and assigning those to the portions of the system desired.

In the case of dynamic service provisioning, remember that the switch is empowered to deliver any of the existing Roles as defined in Policy Manager. When the switch decodes the authentication response from the RADIUS server, it checks the Filter ID field, reads the Role value, and configures that port with the appropriate policy settings. This includes the introduction of the appropriate Classification Rules on that particular interface. This process ensures that users that authenticate in the User Personalized Network system are granted secure access to the appropriate network resources, at the appropriate service levels.

Now that all four stages of the User Personalized Network have been described, the point has been reached at which the users of a network system have secure access to the Services that enable them to perform their job function securely and reliably. It is interesting to note that if the system is configured correctly, the user doesn't actually know that the policy rules have been applied, unless they attempt to violate those rules. Often, though, even during violations the user would not know that the policy rules existed. Consider the case of Napster, one of the most pervasive applications of the day. If a user was logging in to Napster to download music, they could potentially consume a great deal of bandwidth. If that application is denied access to the network, which is possible, the users would certainly find a way to log back in at some point in the future, by changing the way the application looks and behaves on the network. On the other hand, if that same user is allowed to log in to Napster, but their traffic is limited to X amount of bandwidth, or is prioritized lower than mission critical data, the user continues to use the application and does not look for ways to "get around the system." This is the kind of solution that doesn't restrict the users from being creative, or expanding the ways they use the network, but it does ensure that creativity doesn't come at the expense of the success of the business operation. After all, it is the decision of the administration to decide how strict the policy rules are, and where, how and when they are applied. It is the role of the IT system to provide them the opportunity them to do that.

Deployment of the User Personalized Network System

It has been mentioned that the User Personalized Network system is functionally modular, and that the components are independent of each other. This is an important competitive advantage for Enterasys because it allows the system to adapt to changes and implement emerging standards without impacting the other components of the system.

The deployment of the User Personalized Network is also likely to be best implemented incrementally, to ensure that the desired result is achieved at each stage, and can be certified over time. As a result, the likely deployment of the User Personalized Network will occur in a few phases, designed to ensure that the system is deployed successfully. Each phase may be viewed as a step in the progression or, if the desired result is achieved, the end of the process. There are no restrictions as to how the system is deployed, as it is a framework, designed to allow each implementation to be customized to best serve the demands of a given deployment. The phases are likely to be:

- Creation of the Relationship Hierarchy
- Enabling of Authentication in shared areas, and specific cases
- Wide scale deployment of authentication and dynamic policy

Creation of the Relationship Hierarchy

The implementation of NetSight Policy Manager provides an excellent opportunity to make some determinations about the behavior of the network, and the desired experience afforded to the users that conduct business over that network. It is, therefore, advisable that the development of the Relationship Hierarchy be performed with care, and accuracy, to ensure the desired result.

The first Roles to be constructed are likely to be those of the default system behavior. This allows the network to deliver the appropriate levels of service to the system, in particular, static devices such as printers, servers, and legacy network infrastructure components, and to secure the network against many kinds of attacks, both malicious and unintentional. Default Roles can also be used to provide basic network connectivity either prior to, or in the absence of, authentication. Subsequent construction of Roles to be assigned dynamically can occur incrementally as well. The first Roles to be created, and assigned dynamically are likely to be simple, yet purposeful. These will include Roles such as Internal and External, where only those in possession of valid username and credentials will have access to the corporate resources. Subsequent Role development will be performed to incrementally to improve the system, and insure greater security and more granular control of network resources.

Enabling of Authentication in Shared Areas, and Specific Cases

It is likely that the first deployments of LAN-based authentication will occur in areas where special security considerations warrant its use. These include shared areas such as conference rooms and areas where wireless network access points provide wireless connectivity to the network. Additionally, there are groups of users that are candidates for early deployment of authentication as well, such as consultants, temporary employees, and contractors. The idea is for the IT support staff to get accustomed to administering a system in which the failure to authenticate has different results than currently occur. While the result is certainly a more secure network, the administration of that network requires a slightly different approach than has historically been the case.

Wide Scale Deployment of Authentication and Dynamic Policy

In many large enterprises, it will be highly desirable to deploy the combination of static and default policy, as well as large-scale deployment of authentication and dynamic policy. In these deployments, tight integration with the desktop operating system, username and credentials databases, and directory components, ensures that the greatest benefits are realized with the least exposure to risk. In this scenario, network security is greatly improved due to number of technological enhancements including:

- The introduction of authentication at the closest possible point to the user
- Users cannot access information that is not applicable to their job function
- Visitors can no longer access either the wired or wireless network without the appropriate username and credentials
- Attacks against network infrastructure devices are greatly reduced, if not eliminated due to the inability of potential attacker to access the protocols, devices, or network bandwidth required to launch such an effort

These kinds of drastic improvements significantly improve the ability for businesses to gain a competitive advantage in their market space. This, after all, is the ultimate goal of the IT department in today's rapidly changing business climate.

Conclusion

In the User Personalized Network, Enterasys has developed a solution that allows the IT department to align the work that they do with the goals of the organization. This will certainly have an identifiable impact on the kinds of projects that get funded in the coming years, and will also increase the success ratio of IT initiatives. In a market congested with schemes to deliver network policy, Quality of Service, and increased security, the Enterasys User Personalized Network system stands alone in its ability to align the goals of the business with the capabilities of the IT system. It achieves this by allowing non-technical as well as technical members of the organization to have a voice in the deployment of business critical network Services. It is a combination of innovation in software, sound architectural design in infrastructure gear, and a continuing commitment to driving and supporting industry standards.

The User Personalized Network is the result of a company investing the time to understand the challenges its target market is facing, and creating solutions to address those challenges. It is the product of Enterasys Networks, a company focused on delivering business-focused solutions that allow clients to realize a competitive advantage through IT.

North America

35 Industrial Way
Rochester, NH 03867
U.S.A.
(603) 332-9400

50 Minuteman Road
Andover, MA 01810
U.S.A.
(978) 684-1000

Europe/Middle East/Africa

Network House
Newbury Business Park
London Road, Newbury
Berkshire, England RG13 2PZ
44-1635-580000

Asia Pacific

85 Science Park Drive
#03-01/04
The Cavendish
Singapore 118259
65-775-5355

Unit 8,Allambie Grove Estate
25 Frenchs Forest NSW 2086
Sydney, Australia
61-29950-5900

Latin America

Periferico Sur No. 3642
Piso 6
Colonia Jardines del Pedregal
Mexico City DF 01900
Mexico
525-490-3400

Av Jurubatuba, 73-3° andar
Brooklin-São Paulo
04583-100-Brazil
55-11-5508-4600