# Global Information Assurance Certification Paper

# Cisco PIX Authentication and Cisco SecureACS

Scott Jensen
April 6, 2002

## Introduction

Many organizations today are creating Internet accessible Web Servers that are designed for use only by their employees. One popular use is Web-enabled electronic mail that can be accessed by employees anywhere they have access to an Internet connection. As e-mail has become a primary means for communication, Web-enabled e-mail can be an incredible productivity tool. This is especially true for those organizations that support the road warrior or encourage telecommuting among their employees.

Web access to one's e-mail account is generally protected only by a userid and password. For those who administer a Novell GroupWise system, it's common knowledge the password is notoriously weak. GroupWise places no requirement for a minimum number of characters nor can time expirations be forced. Essentially, a GroupWise user can have a one-character password that they never have to change. Now that's lousy security!

As can be seen, while Web-enabled e-mail is both convenient and productive for the end user, it also presents considerable security concerns for the network administrator. For that reason, a security-conscious organization should consider creating an added layer of authentication protection

For those organizations that utilize the Cisco PIX firewall, this document will introduce the authentication capability of the PIX firewall and Cisco's Secure Access Control Server (SecureACS) for WindowsNT and Windows 2000. Version numbers are 6.1 for the PIX firewall and 2.6 for SecureACS.

## Cisco PIX AAA Support

The Cisco PIX firewall offers support for AAA services, or Authentication, Authorization and Accounting.

> *Authentication* requires a user to prove they really are who they say they are. Methods of authentication can be username and password, challenge/response, one-time password, token card and other methods.
>
> *Authorization* services decide which resources the user is allowed to access and which operations the user is allowed to perform.
>
> *Accounting* records what the user actually did, what they accessed, and how long they accessed it.

Cisco touts the PIX firewall provides the fastest method for a firewall to authenticate a user with a technology referred to as cut-through proxy authentication. The PIX firewall gains dramatic performance advantages through cut-through proxy, a patent-pending method of transparently verifying the identity of users at the firewall and permitting or denying access to any TCP- or UDP-based application. Unlike a proxy server, which must analyze every data packet at the application layer of the Open System Interconnection (OSI) model (a time- and process-intensive function), a PIX firewall first queries a TACACS+ or RADIUS database server for authentication. When a user is approved and policy is checked, the Cisco Secure PIX firewall series shifts the session flow, and all traffic thereafter flows directly and quickly between the two parties while session state information is maintained. This cut-through proxy capability allows the Cisco Secure PIX firewall series to perform dramatically faster than proxy servers.

The PIX firewall supports two primary security server protocols: RADIUS and TACACS+.

RADIUS (Remote Access Dial-In User Service) can probably be considered the defacto standard for AAA services because it is an open protocol system widely supported in products by many different vendors. In addition there are many vendors that produce RADIUS compliant security servers. The RADIUS protocol is defined in RFC 2865 and RADIUS in RFC 2866.

TACACS+ (Terminal Access Controller Access Control System) was introduced by Cisco as an enhanced version of the existing TACACS protocol as described in RFC1492. TACACS+ has not yet been ratified by the IETF and is generally used only between Cisco and compatible products.

TACACS+ offers some advantages over RADIUS such as: TCP transport protocol (RADIUS communicates over UDP), separation of the three AAA services (RADIUS combines authentication and authorization), and data integrity encrypting the entire packet (RADIUS encrypts only the password). If possible and especially if utilizing Cisco products, TACACS+ should be the AAA protocol of choice.

**Cisco SecureACS**

The SecureACS software is Cisco's implementation of the AAA security server. While the Windows version will be discussed in this paper, a version for UNIX is also available.

SecureACS offers centralized access control and supports both the RADIUS and TACACS+ protocols. It supports not only the PIX firewall as described here but all Cisco network access servers. In addition, it can also be utilized to control other forms of access such as Telnet access to routers and switches.

Like most AAA security servers, SecureACS allows the administrator to create and maintain a local database of users from which to perform authentication and authorization services. In addition to the local database, SecureACS also allows the administrator to authenticate a user utilizing a variety of external user databases. In version 2.6, external database support includes:

- Open Database Connectivity (ODBC)
- Generic LDAP
- Microsoft Commercial Information Server (MCIS)
- CRYPTOCard
- SafeWord
- AXENT
- Security Dynamics/RSA
- Novell NetWare Directory Services (NDS)
- Windows NT/2000 User Database

The Sophisticated Unknown User Handling (as it's known) feature enables SecureACS to contact these external databases instead of, or in addition to, its own internal database to authenticate incoming and outgoing user requests. Because the username and password of users can be authenticated against these external authentication databases, there is no need for the network administrator to manually maintain a duplicate list within Cisco Secure ACS. In a large organization, this can greatly reduce administrator overhead . In addition, external database support allows the organization to take advantage of the inherent security features present in enterprise-scale user and directory databases such as WindowsNT and Novell NDS.

**PIX AAA Configuration**

As described previously, the PIX firewall supports all facets of AAA. The configuration examples presented in the following sections will concentrate primarily on the authentication function of AAA.

The first set of commands are necessary to define what protocol will be used to communicate between the PIX firewall and the AAA server as well as to identify the AAA server.

```
aaa-server TACACS+ protocol tacacs+
aaa-server auth-serv protocol tacacs+
aaa-server auth-serv (inside) host 10.0.0.1 shared secret  timeout 20
```

The aaa authentication command is used to define what and who will be subject to authentication. There are numerous operator combinations available with the aaa authentication command. This provides a great deal of flexibility in satisfying the security needs of a particular organization. Authentication can be forced on either **inbound** or **outbound** connections (inbound identifies connections from a lower to higher security interface, outbound from a higher to lower security interface). Authentication can be forced for a particular TCP/UDP service or for all TCP/UDP services. In addition, authentication can be required for a particular source or destination network or host address. All the following examples illustrate connections from any source address (0.0.0.0) to any destination address (0.0.0.0).

```
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0 auth-serv
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 auth-serv
aaa authentication include http inbound 0.0.0.0 0.0.0.0 auth-serv
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0 auth-serv
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 auth-serv
```

```
aaa authentication include http outbound 0.0.0.0 0.0.0.0 auth-serv
```

The next two examples will force authentication on any protocol (TCP or UDP) attempting access through the firewall. The administrator may decide to use this configuration in an environment when there are a number of different ports open on the PIX firewall and they want to ensure authentication is passed before any access is permitted.

```
aaa authentication include any inbound 0.0.0.0 0.0.0.0 auth-serv
aaa authentication include any outbound 0.0.0.0 0.0.0.0 auth-serv
```

In a situation where the administrator has configured the PIX firewall to force authentication for all TCP traffic, there may quite likely be a protocol for which authentication is not desired. For instance, an SMTP server must be allowed to send and receive e-mail through the PIX firewall without being forced to authenticate. In these cases, the PIX firewall provides the **exclude** operator.

```
aaa authentication exclude tcp/25 outside 10.0.0.8 255.255.255.255 0.0.0.0 auth-serv
```

The above statement allows SMTP traffic sent from the outside to host 10.0.0.8 on port 25 to be excluded from the authentication requirement.

At this point, it is important to note the PIX firewall can authenticate only **FTP, Telnet and HTTP** connections. This presents a problem when the administrator has configured the PIX firewall to authenticate all connections. How can these other connections be authenticated? There is a technique referred to as **Virtual Telnet** that will allow the PIX firewall to authenticate other protocols. Use the following command.

```
virtual telnet 192.168.2.1
```

The users will simply telnet to the advertised IP address where they are presented with the same authentication credentials. Once the user has established PIX firewall authentication by accessing the virtual telnet service, they are then permitted to utilize other services permitted by the PIX firewall access control lists (discounting any AAA authorization restrictions).

Finally, authentication timeouts should be configured. An authentication timeout will automatically remove the authentication credentials from the PIX firewall after a period of either inactivity or a specified duration. The first timeout command specifies authentication timeout after 30 minutes of inactivity. The second timeout command specifies authentication timeout 30 minutes after authentication was granted regardless of user activity.

```
timeout uauth 0:00:00 absolute uauth 0:30:00 inactivity
timeout uauth 0:30:00 absolute uauth 0:00:00 inactivity
```

**SecureACS Configuration**

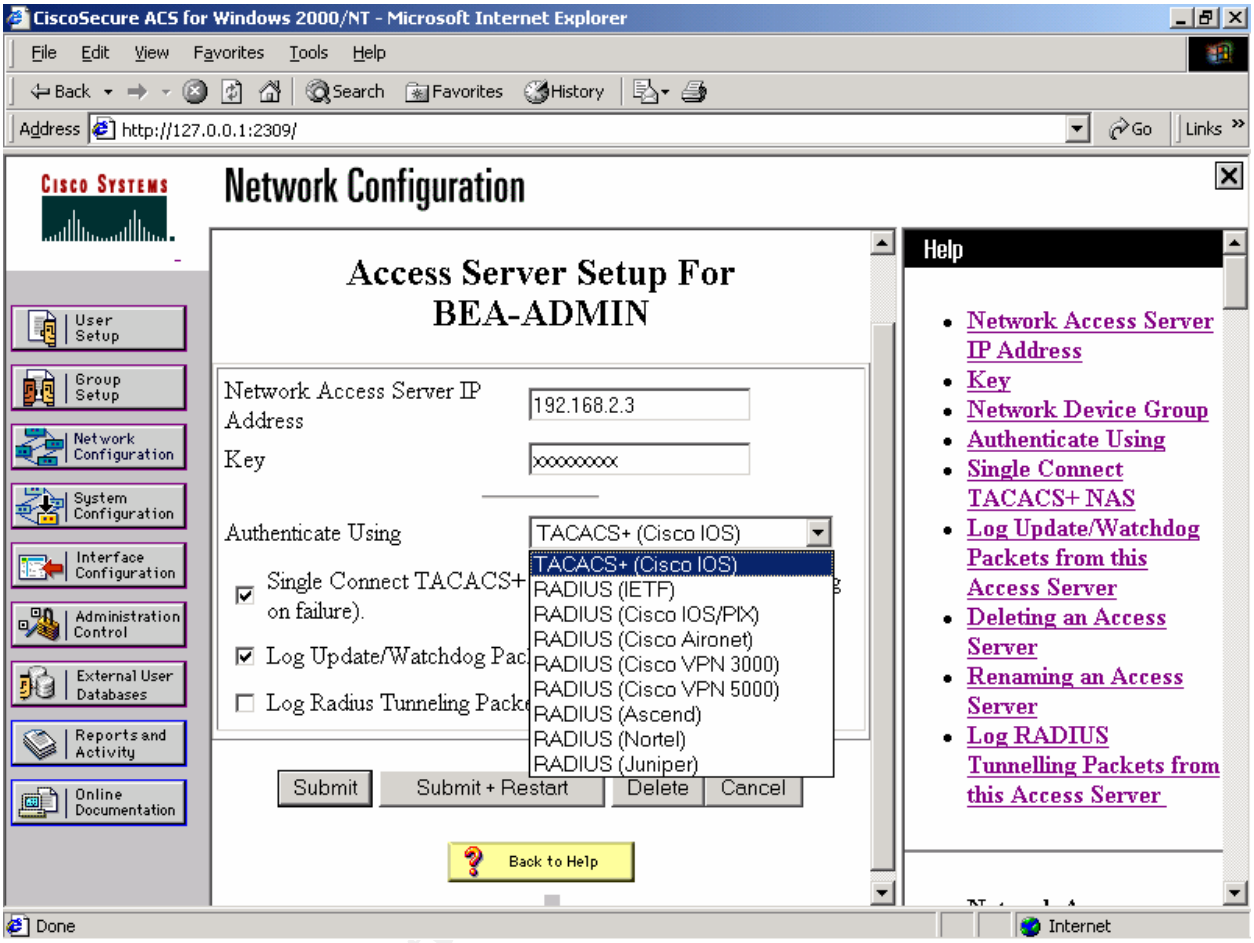
As discussed previously, SecureACS has the capability to authenticate a user session against either a local database or a variety of external user databases. The following will present a

minimal configuration of SecureACS to interface with Novell's Netware Directory Services for authentication credentials.

Note: In order for SecureACS to utilize the NDS database, the Netware Client must be installed on the WindowsNT/2000 server where SecureACS is installed. As of this writing, version 4.83 is the latest Netware client and should be used.

SecureACS utilizes a standard browser such as Netscape or Internet Explorer and is very easy and intuitive for the administrator to understand and configure. From the main screen, the administrator not only has ready access to all areas of server configuration, but also can easily review RADIUS and TACACS+ reports and activity. In addition, online documentation is also available (important as SecureACS does not include any paper documentation).

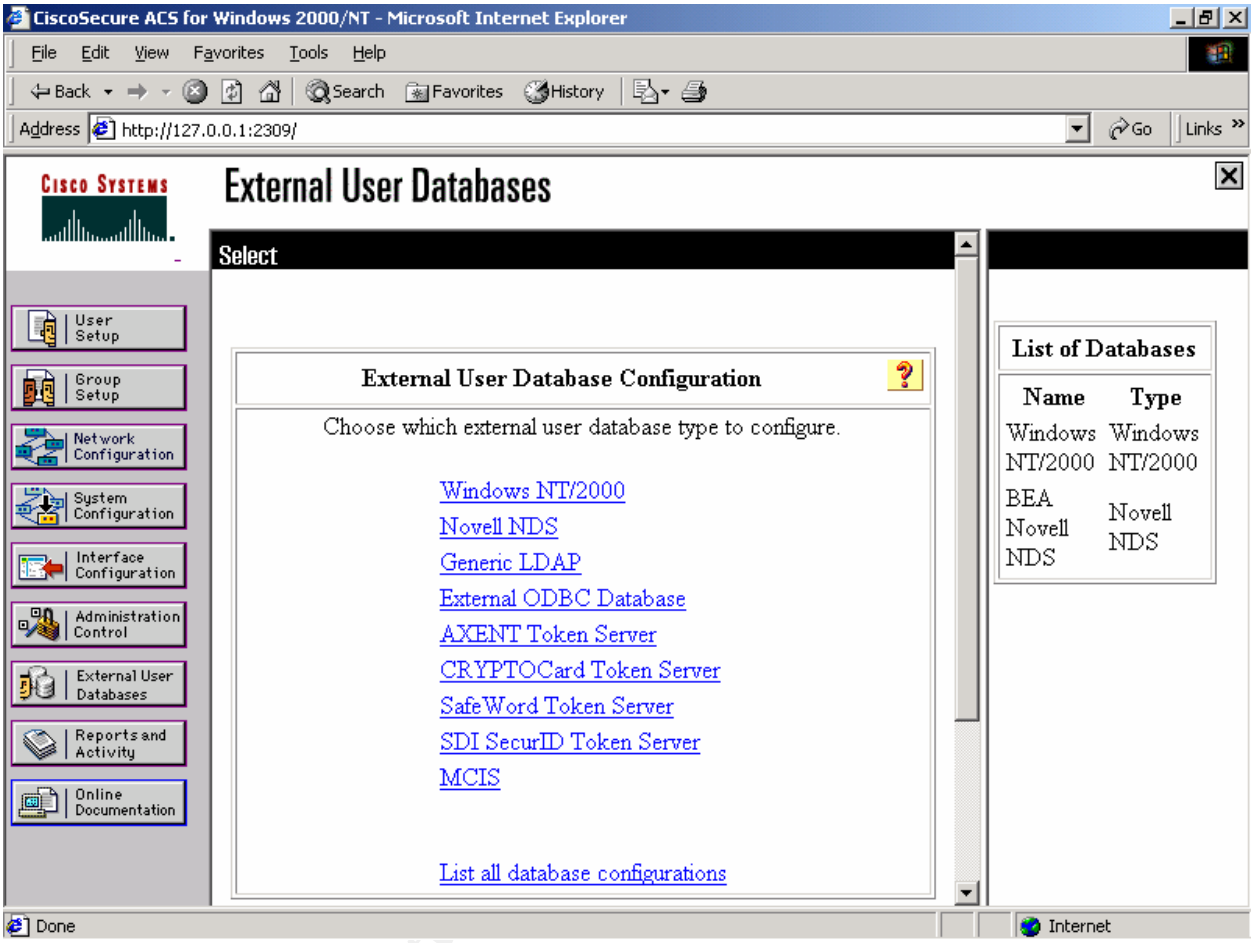
Defining the PIX firewall to SecureACS is the first step in the configuration process. Creating a new Access Server within the Network Configuration button will accomplish this. In this slide, the PIX firewall was named BEA-ADMIN.




Enter the IP address of the PIX firewall interface accessible to SecureACS, and the shared secret key that will be used to authenticate communications between the PIX firewall and SecureACS.

As the PIX firewall has previously been configured to utilize TACACS+ as the AAA protocol, be sure to select this entry from the Authenticate Using drop down menu.

The next step is to configure SecureACS for external database authentication support in addition to the local SecureACS database. As we will be using Novell NDS, select this option from the External User Database window.

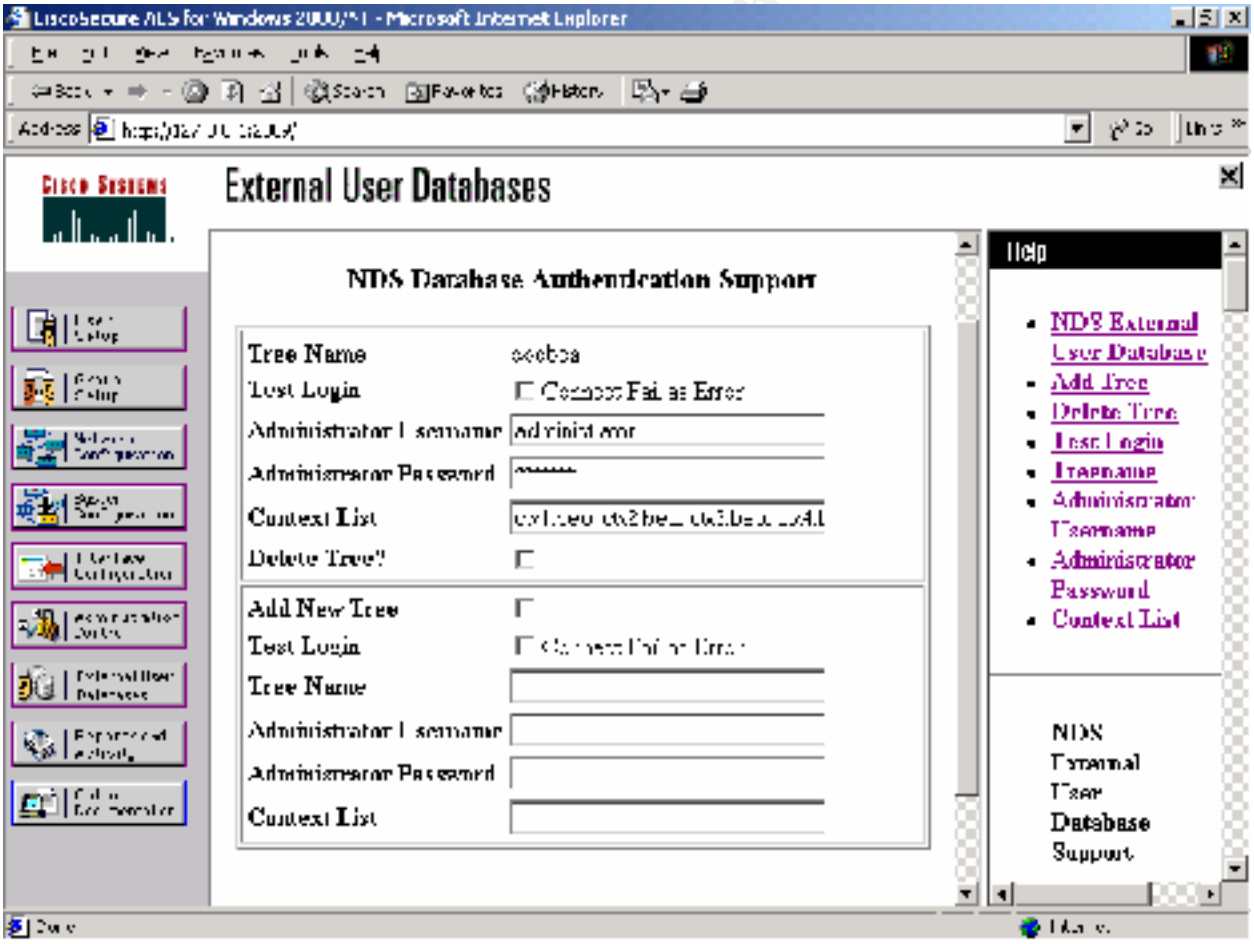


Before the following screen actually appears, you will be asked to give a descriptive name for the NDS Tree. In this slide, the tree name entered previously is “docbea”.

The Administrator Username must be an NDS user that has Supervisor rights to the NDS tree in question. Enter the password for the administrator account.

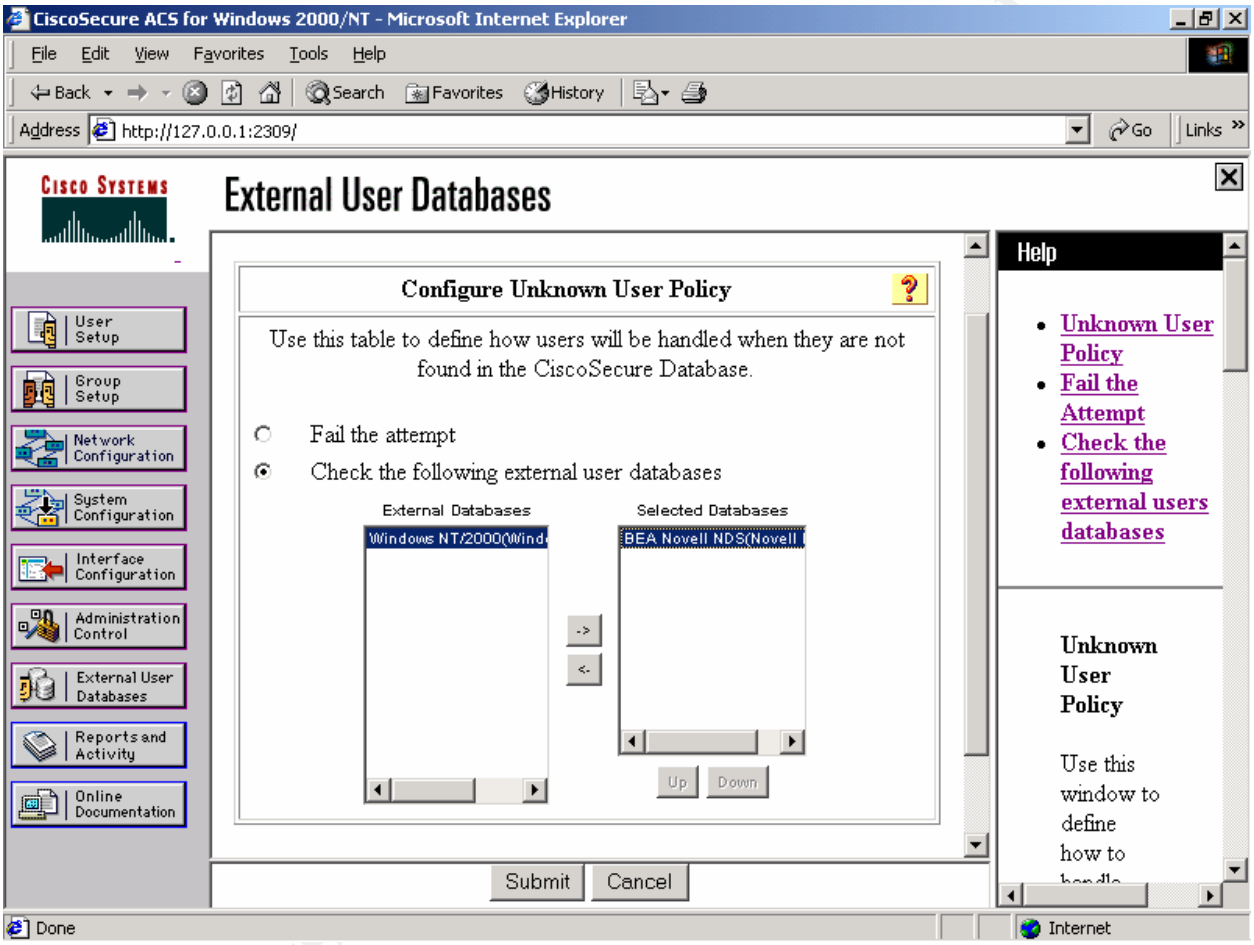
In order to simplify authentication for the remote user, the Context List field should define each context within the NDS tree for which a remote user may reside. If a context for a particular user does not reside within this field, the remote user must enter their distinguished name in order to authenticate. Since many users have no idea what their actual context is, entering their context here allows them to enter their common name only.

However, an alternative school of thought is that requiring the distinguished name for authentication may decrease the likelihood of guessing a weak common name. Separate contexts with a comma.



Finally, configuration of the Unknown User Policy must be completed. As can be seen, when SecureACS cannot find a user in the local database, the server can either fail the attempt or check an external user database.

Since we want NDS checked, we select the Novell NDS database that was defined previously be checked for existence of the authenticating user.




After completing these configuration steps for the PIX firewall and SecureACS, a user should be able to successfully pass PIX firewall authentication using their Novell NDS userid and password.

Please note these are only minimal configurations. The needs of your organization may require substantial fine-tuning of the process to achieve optimal results.

**Houston, We Have A Problem**

As is often the case with real life, things do not always work as expected once a design moves from a test to a production environment. This is especially true when the Internet is involved. There have been a couple "gotcha's" the author has faced in a production environment that bear mentioning should the reader find themselves in a similar situation. This particular environment is like that discussed during the introduction component of this paper. A Microsoft IIS web server was installed for web based access to an internal electronic mail system and placed on a DMZ interface of the PIX firewall. A certificate was installed on the server for encrypting communications utilizing secure sockets layer running on standard HTTPS port 443. Authentication at the PIX firewall was required before being granted access to the web server. An additional userid and password was then required to access one's e-mail account.

In this environment, the administrator knew the PIX firewall was only capable of authenticating HTTP access to the web server, not HTTPS. That being the case, the decision was made to require authentication for all inbound traffic, thus preventing unauthenticated access over the SSL protocol. As part of this design, the web server home page required HTTP only which allowed the remote user to properly authenticate to the PIX firewall. A link from the home page switched session flow to HTTPS for accessing the remainder of the web site. HTTPS was a requirement for access to all areas of the web server other than the default home page.

Before proceeding, some background information is necessary to explain how the PIX firewall authenticates a particular host connection through the firewall. When a user (or host machine) has successfully authenticated to the PIX firewall, a table of authenticated users and their respective host IP address is maintained on the PIX firewall. This information can be viewed using the **show uauth** command from the PIX firewall command line.

```
PIX-FW1# sh uauth
                    Current    Most Seen
Authenticated Users     1          11
Authen In Progress      0          5
user 's_smith' at 192.168.3.4, authenticated
    absolute timeout: 0:00:00
    inactivity timeout: 0:21:00
PIX-FW1#
```

The authenticated host IP address will be tracked for the remainder of the TCP session by the PIX firewall. The PIX firewall will verify that the source address of all ensuing incoming packets matches information in the uauth table (either for this particular authenticated user or others in the table). If a source address does not match one existing in the uauth table, the packet is either discarded as violating the authentication rule or authentication is requested for a new session.

**Problem Issue One**

The following are contiguous Microsoft IIS log entries showing communication between a client machine and the IIS Web Server (10.0.0.5). Time stamps and other superfluous information have been removed for clarity and compactness. Source IP address changed to private space.

192.168.10.10 - 10.0.0.5 80 GET /login/Default.htm - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 80 GET /login/waslogo.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 80 GET /login/dotzero.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 80 GET /login/novellred.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 80 GET /login/logonlf.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 80 GET /login/images/dotzero.gif - 404 Mozilla/4.0
192.168.10.10 - 10.0.0.5 443 POST /scripts/NSGISAPI.dll webacc^/servlet/webacc 200 Mozilla/4.0
192.168.10.10 - 10.0.0.5 443 GET /com/novell/webaccess/images/dotzero.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 443 GET /com/novell/webaccess/images/waslogo.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 443 GET /com/novell/webaccess/images/novellred.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 443 GET /com/novell/webaccess/images/btnloginen.gif - 304 Mozilla/4.0
192.168.10.10 - 10.0.0.5 443 GET /com/novell/webaccess/images/btnhelpen.gif - 304 Mozilla/4.0

As can be seen, in all communications between the client and web server the client IP address remains consistent, whether accessing the server via port 80 or port 443. This represents a successful connection between the client and web server after authentication to the PIX firewall.

In a production environment, it was discovered that some Internet Services Providers (normally of the dial-up variety) do not maintain a consistent source address for all TCP connections.

The following are contiguous Microsoft IIS log entries showing communication between another client machine and the same IIS Web Server. This particular client was connected to the Internet via the ISP Starpower/RCN. Time stamps and other superfluous information have been removed for clarity and compactness. Source IP address changed to private space. In this example, the IP address assigned to the client machine upon connection to the ISP was 172.25.16.5. Note: PIX authentication was disabled while producing these log entries.

192.168.15.10 - 10.0.0.5 80 GET /login/ - 302 Mozilla/4.0
192.168.15.10 - 10.0.0.5 80 GET /login/Default.htm - 200 Mozilla/4.0
192.168.15.10 - 10.0.0.5 80 GET /login/waslogo.gif - 200 Mozilla/4.0
192.168.15.10 - 10.0.0.5 80 GET /login/dotzero.gif - 200 Mozilla/4.0
192.168.15.10 - 10.0.0.5 80 GET /login/novellred.gif - 200 Mozilla/4.0
192.168.15.10 - 10.0.0.5 80 GET /login/images/dotzero.gif - 404 Mozilla/4.0
192.168.15.10 - 10.0.0.5 80 GET /login/logonlf.gif - 200 Mozilla/4.0
172.25.16.5 - 10.0.0.5 443 POST /scripts/NSGISAPI.dll webacc^/servlet/webacc 200 Mozilla/4.0
172.25.16.5 - 10.0.0.5 443 GET /com/novell/webaccess/images/waslogo.gif - 304 Mozilla/4.0
172.25.16.5 - 10.0.0.5 443 GET /com/novell/webaccess/images/dotzero.gif - 304 Mozilla/4.0
172.25.16.5 - 10.0.0.5 443 GET /com/novell/webaccess/images/novellred.gif - 304 Mozilla/4.0
172.25.16.5 - 10.0.0.5 443 GET /com/novell/webaccess/images/btnloginen.gif - 304 Mozilla/4.0
172.25.16.5 - 10.0.0.5 443 GET /com/novell/webaccess/images/btnhelpen.gif - 304 Mozilla/4.0

Notice the source IP address is different when the client communicates via HTTP port 80, presumably the result of network address translation. When the client attempts a connection using a protocol other than HTTP (in this case SSL port 443), the source IP address reverts to the

client's actual IP address. In this situation, the end user received a browser "page not found" error when attempting to access the SSL portion of the web site. Why?

The PIX firewall initially authenticated the client as 192.168.15.10. As soon as the client attempted to access the web site via SSL, the source IP address changed. The PIX firewall detected this as an unauthenticated IP address and blocked the connection for that user. Not good.

The solution to this problem was to have users of Starpower/RCN utilize the virtual telnet feature of the PIX firewall described previously. Again, when the client used a protocol other than HTTP, the IP address change did not occur. In this case, telnet fit the bill. Once authentication was granted for the client (IP address 172.25.16.5), they bypassed the default home page and proceeded directly to the SSL protected area of the web server, completing a successful session. At no point, was HTTP utilized when accessing the web server.

America Online presented a slightly different spin on the same HTTP problem for the PIX firewall. Similar to Starpower/RCN, AOL will utilize not only one different source IP address when the client communicates via HTTP, but connections to a web server may come from several different source IP addresses. This made for interesting authentication reports from SecureACS. However, it was discovered this trend only occurs when the client used the built-in AOL browser. If the client simply connected to AOL, then used a separate browser such as Netscape or Internet Explorer, the problem with the varying source IP address did not occur. Authenticated communications via the PIX firewall worked as designed.

Illustrating the above, the following are contiguous Microsoft IIS log entries showing communication between an AOL client machine and the same IIS Web Server. The built-in AOL browser was used. Again, time stamps and other superfluous information have been removed for clarity and compactness. Source IP address changed to private space. Note: PIX authentication was disabled while producing these log entries.

```
172.16.97.13 - 10.0.0.5 80 GET /login/ - 302 Mozilla/4.0
172.16.96.200 - 10.0.0.5 80 GET /login/Default.htm - 304 Mozilla/4.0
172.16.96.204 - 10.0.0.5 80 GET /login/waslogo.gif - 304 Mozilla/4.0
172.16.96.236 - 10.0.0.5 80 GET /login/dotzero.gif - 304 Mozilla/4.0
172.16.97.14 - 10.0.0.5 80 GET /login/novellred.gif - 304 Mozilla/4.0
172.16.97.9 - 10.0.0.5 80 GET /login/images/dotzero.gif - 404 Mozilla/4.0
172.16.96.205 - 10.0.0.5 80 GET /login/logonlf.gif - 304 Mozilla/4.0
```

Attempts to contact both Starpower/RCN and AOL to determine the reasons behind their practice of selected source IP address alteration were not successful.

**Problem Issue Two**

The second issue regards how SecureACS communicates with Novell's NDS when attempting external database authentication. When SecureACS receives an authentication request from the PIX firewall for a user located within NDS, it will utilize the configured administrative account to quickly verify the userid and password forwarded from the PIX firewall.

Because of the lack of Cisco documentation stating otherwise, it was assumed there was not an actual logon attempt made by SecureACS on behalf of the user against the NDS tree. In further support of this hypothesis, the last access time for a particular NDS user after a SecureACS authentication did not indicate a corresponding recent logon.

This theory was challenged when a user of the system complained of only one Novell grace login after returning to the office after a weekend in which they accessed the web server on a couple occasions. Novell grace logins occur when a password has expired and allow a user *x* number of additional logins without being forced to change their password. Once grace logins are exhausted, the user will no longer be able to login without a password reset. The NDS tree in this organization is configured to allow 4 grace logins for a user once their password has expired. This user's password had expired over that particular weekend.

Subsequent testing of the process showed that when a user's NDS password expired and external NDS database authentication via SecureACS was granted, the grace login parameter was decremented by one each time SecureACS authentication process took place. Given enough authentication attempts, the grace login parameter would eventually reach zero. At that point, the user would not be able to complete a successful login to the network from the office once they return.

The last statement was worded "from the office" intentionally. The other interesting aspect to this behavior was that the user was still able to access the PIX/SecureACS protected web server using their expired password even after all NDS grace logins were exhausted. Cisco technical support personnel could not explain this fact.

**Conclusion**

In the future, demand for remote Internet access to extranets and other web-based productivity applications by employees and partners alike will certainly continue to rise. Security conscious organizations should require some level of authentication to protect access to corporate information.

While application level authentication is and should be used, multiple layers of authentication are always a good idea. Authentication at the firewall provides a strong first layer of access control for these internal systems.

For those organizations that have settled on the PIX firewall platform and require AAA services, Cisco SecureACS makes an excellent choice due to it's ease of use, scalability, external user database support and excellent integration with the PIX firewall.

**References**


Wenstrom, Michael. Managing Cisco Network Security. Indianapolis: Cisco Press, 2001

Cisco. "Cisco PIX 500 Firewalls". 2002. URL: http://www.cisco.com/go/pix (March 8, 2002).

Cisco. "Overview, Cisco Secure PIX firewall Series". December 12, 2000. URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix_pa.htm (March 22, 2002)

Cisco. "How to Perform Authentication, Authorization, and Accounting of Users Through the PIX (5.2 Through 6.1)". Document ID 8527. February 26, 2002. URL: http://www.cisco.com/warp/public/110/atp52.html (March 22, 2002).

Cisco. "Cisco Secure Access Control Server". 2002. URL: http://www.cicso.com/go/acs (March 8, 2002)

Cisco. "Novell NDS Database Authentication Configuration". Step-by-Step Configuration for Cisco Secure ACS. December 29, 2000. URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt26/usergd26/ch3.htm#xtocid28990129 (March 23, 2002).

Cisco. "Sophisticated Handling of Unknown Users". December 29, 2000. URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt26/usergd26/unknown.htm (March 23, 2002).