Global Information Assurance Certification Paper

Damon Martin
GIAC Certified Windows Security Administrator (GCWN)
Version 3.1 Option C

SECURING CISCO DEVICES USING MICROSOFT INTERNET AUTHENTICATION SERVICE (RADIUS)

INTRODUCTION

With the release of Microsoft Windows 2000 Server came the introduction of Internet Authentication Service (IAS). IAS is a Windows service that allows a Windows based server to provide Remote Authentication Dial In User Service (RADIUS) authentication. The benefit of utilizing IAS to provide RADIUS authentication is that it allows integration with Active Directory (AD) and is available with no additional licensing requirements as part of Windows 2000 and 2003.

The ability to use Windows 2000 to provide RADIUS AAA services for network infrastructure equipment, can allow an organization to integrate active directory authentication and authorization for non-LDAP enabled devices. By configuring Cisco network devices to utilize Microsoft Internet Authentication Service (IAS) for authentication and authorization, network engineers can log onto devices with their Active Directory (AD) user account and password and get specific levels of access based on Windows group memberships.

WHAT IS RADIUS

Ensuring that only the appropriate people or processes are granted access to specific resources in an Information Technology environment is always a critical concern. The combination of Authentication, Authorization and Accounting services, commonly referred to as AAA (pronounced “Triple A”), are designed to provide the foundation for access control. The roles of each component are:

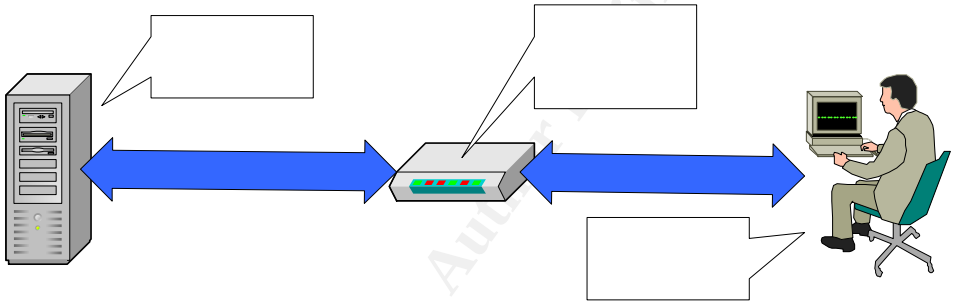
Authentication The act of validating that a person or system is who they claim to be. This generally involves a claim of identity (username) followed by proof of that identity (password). Competition of the authentication process, in itself, does not guarantee a specific level of access

Authorization The process of determining and granting the appropriate level of access given an authenticated identity.

Accounting The process of logging or recording the access granted or denied by a particular system.

RADIUS was developed to provide a solution to the problem of managing AAA services for large modem pools used for dial up access to network systems. The protocol became widely utilized during the 1990's as Internet Service Providers began to grow to the point that it was increasingly difficult to centrally manage authentication of large numbers of users connecting to the modem pools.

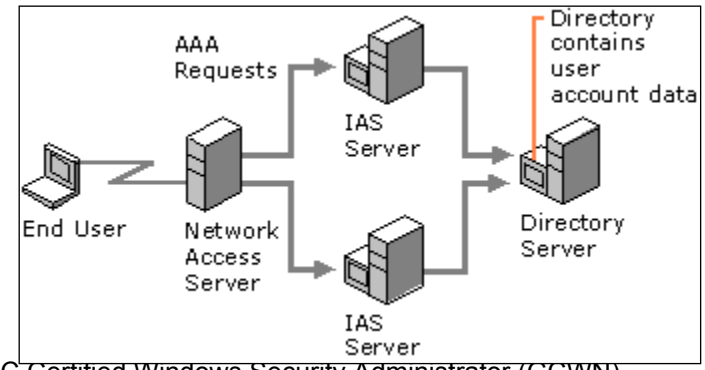
The RADIUS protocol is structured on a client server model. In a RADIUS implementation, the client is the network device that is requesting authentication and/or authorization for a remote user. The RADIUS server is the central system that houses the master list of user accounts, passwords and access rights for the users to be granted access.



One of the key points to understand regarding RADIUS services is that the remote user never forms a connection to the actual RADIUS server. From a security standpoint, the RADIUS client is acting as an authentication proxy by asking for authentication on the user behalf from the RADIUS server. This is an important distinction that will be explained more in depth during the discussion of IAS setup and configuration.

WHAT IS IAS

Microsoft Internet Authentication Service (IAS) is a Microsoft implementation of RADIUS. It is designed to provide RADIUS serves for any device, typically remote access services, that are RADIUS compliant. Because IAS is fully compliant with RADIUS standards in RFC 2138, its structure and design are virtually identical to what you would expect in most RADIUS software.



The major benefit of utilizing IAS over a traditional RADIUS deployment is the ability to utilize the Active Directory user database for AAA. By utilizing IAS as the access control mechanism for a Cisco infrastructure device, we are able to use this functionality and avoid creating a separate user management structure to control access to our networking equipment.

HOW TO CONFIGURE IAS

SYSTEM REQUIREMENT OF IAS

Installation of the IAS service requires Windows 2000 Server or Advanced Server. The service itself requires very little resources. There is no difference in the IAS features based on the version of Windows 2000 Server that is utilized. However, there will be limitations in the release of Windows 2003 Server.

Note: In Windows Server 2003, Standard Edition, you can configure IAS with a maximum of 50 RADIUS network access servers, a maximum of two remote RADIUS server groups, and unlimited users.

CONFIGURATION OPTIONS

When setting up ISA server there are two basic configurations: Stand-alone and Active Directory Integrated

WINDOWS 2000 DOMAIN MODE CONFIGURATION

Configuring an IAS server on a Windows 2000 native mode environment provides the most features for managing remote access with groups. The following is a list of the features that become available when utilizing IAS as part of a native mode domain:

- Remote access policies based on flexible group configurations. This includes the use of Universal Groups for including users from multiple domains into a single remote access policy. This is done with nested groups.
- Ability to utilize User Principal Names (UPNs). This will allow for cleaner integration with existing username conventions where users have become accustomed to entering only there username with no domain context. i.e. jdoe instead of jdoe@mycompany.com or mycompany\jdoe.

In an Active Directory integrated environment, the IAS server is registered as a service in AD and provides authorization and authentication services based on domain user or group information.

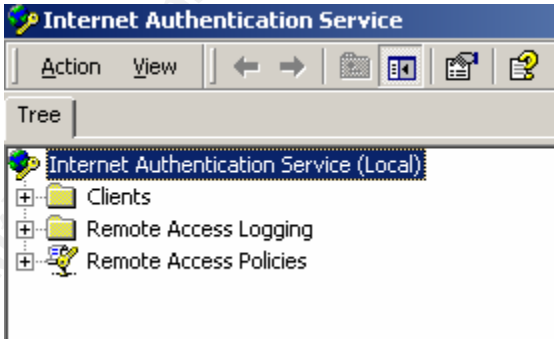
WINDOWS 2000 STAND-ALONE CONFIGURATION

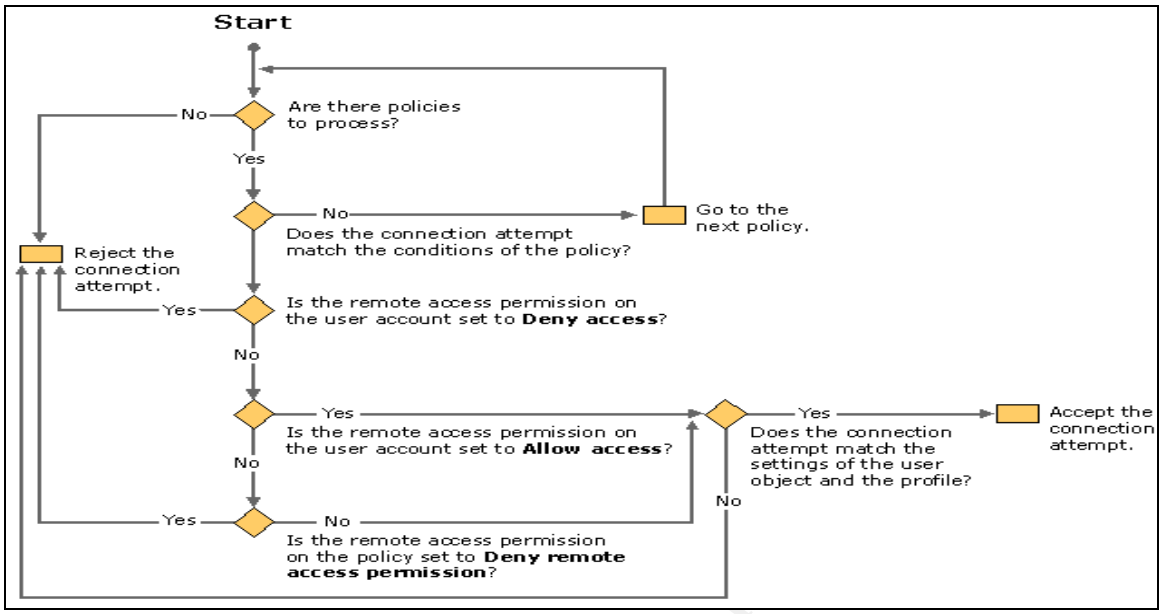
In a standalone environment, the IAS server can reference its local user and group information to provide authentication or authorization services. An IAS server can be configured as a stand-alone service regardless of whether it is a member server in an Active Directory (AD) domain or a stand-alone Windows 2000 Server. That is, a server can be a member of an Active Directory domain and still refer to local accounts for IAS authentication purposes.

Once you have determined whether to utilize IAS Active Directory integrated or stand-alone service the installation process is fairly trivial. Since the direction of this document is to provide AAA services for the Cisco infrastructure equipment on our networks we will utilize an AD integrated environment for examples.

SETTING UP THE SERVICE

In order to be able to better understand how the IAS services processes its authentication requests it is important to look at criteria used by the server. Generally speaking there are three (3) components to the IAS server configuration: Clients, Remote Access Polices and Remote Access Logging. The first step to configuring our IAS server to provide authentication to RADIUS clients like our Cisco network switches and routers is to perform the setup of the IAS sever itself. This is done by opening up the Internet Authentication Service administration console within a Microsoft Management Console (MMC) or from the Administrative Tools folder on the Programs menu. The basic processing of RADIUS requests first confirms that any authorization attempts originate form a valid RADIUS client as configured in the “Clients” section of the console. This authentication is preformed based on the source address for the request and the shared secret. Assuming that the IP address and shared secret correspond to a valid client on the IAS server the following rules are used to process the remote access policies:





Microsoft®

USING RADIUS WITH CISCO EQUIPMENT

BENEFITS OF CENTRALIZED AAA

There are a number of benefits to using centralized AAA services for your Cisco infrastructure equipment. Utilizing IAS enables the granting of network engineers access to specific administrative levels on an entire Cisco infrastructure from a single user database i.e. Active Directory. This will allow for role or group based security used for other network systems to be leveraged by your Cisco infrastructures.

BEST PRACTICES FOR AAA AND CISCO EQUIPMENT

Generally, best practices for implementing AAA on Cisco equipment mandates you address the following capabilities:

- Multiple Privilege levels for various types of user roles
- Secure authentication processes (i.e. password and/or username encryption)

CISCO HARDWARE AND IOS REQUIREMENTS FOR RADIUS

The requirements for utilizing RADIUS on Cisco routers and switches are as follows:

- Routers with Cisco IOS 11.1 and greater support both RADIUS and TACACS+
- Cisco Catalyst IOS based switches with IOS version 12.1(T)

DEPLOYING IAS FOR CISCO EQUIPMENT

WINDOWS 2000 CONFIGURATION

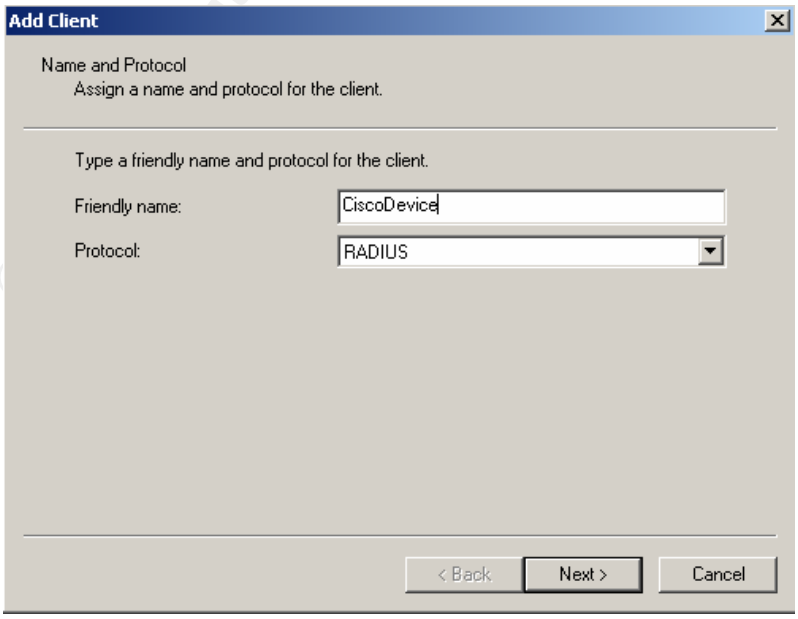
In order to configure a Windows 2000 Server to act as an Internet Authentication Service (IAS), or RADIUS, server the service must be installed as described in the preceding section. Once that is completed you are ready to begin the setup of IAS. The basic structure of RADIUS services consists of three components: RADIUS Clients, the RADIUS server and remote users. In order to understand how these services interoperate, it is important to remember that the IAS server is the authentication server and the Cisco networking equipment is the RADIUS client. The user's logon attempt is "proxied" by the Cisco router or switch. The IAS server has no knowledge of where the users are physically or logically located in the your network environment. The benefit to this configuration is the ability to limit the devices that are allowed to receive authentication services from IAS on a device by device basis.

INSTALLING THE SERVICE

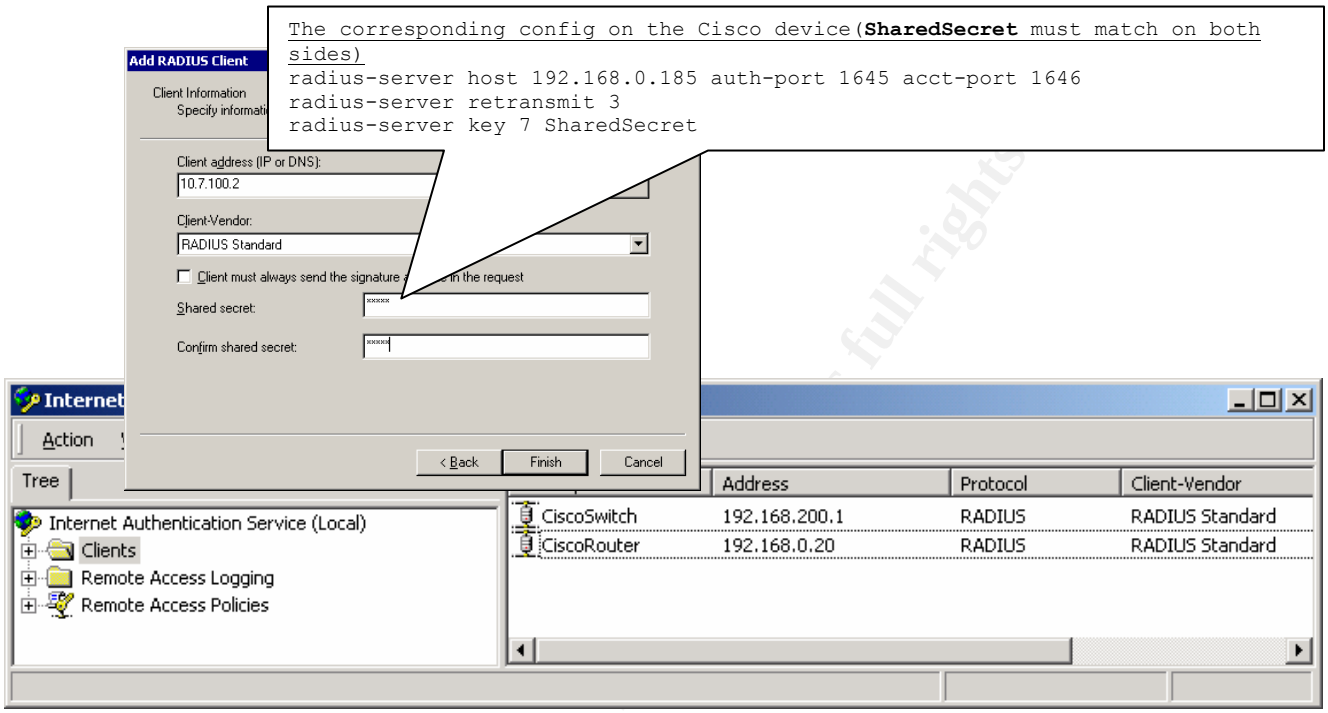
In order to install the service, navigate to the "Add or Remove Programs" applet in the control panel of the Windows 2000 server on which you wish to install the service. From the "Windows Components" Select the Internet Authentication Service and click OK. This will install the needed files and start the service. *A reboot of the server is not required.*

CONFIGURING IAS

1. Open up the MMC for the IAS service and connect to the server.
2. Select Clients from the containers in the left pane. Right-click on the Clients Container and select New | Client. Assign the client a descriptive name and select RADIUS as the protocol.

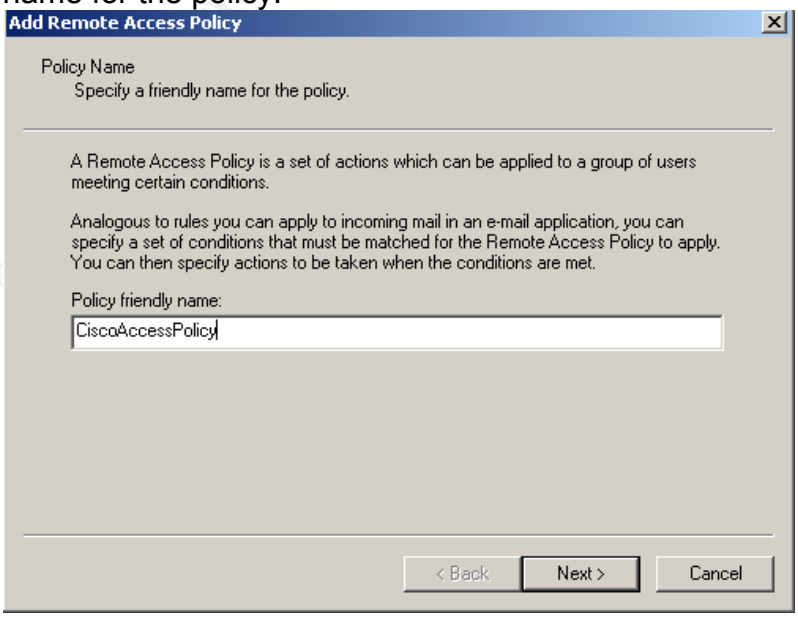


3. Enter the IP Address of the RADIUS client (Cisco device) and the shared secret that will be used to authenticate the RADIUS client (Cisco Device) to the IAS server.

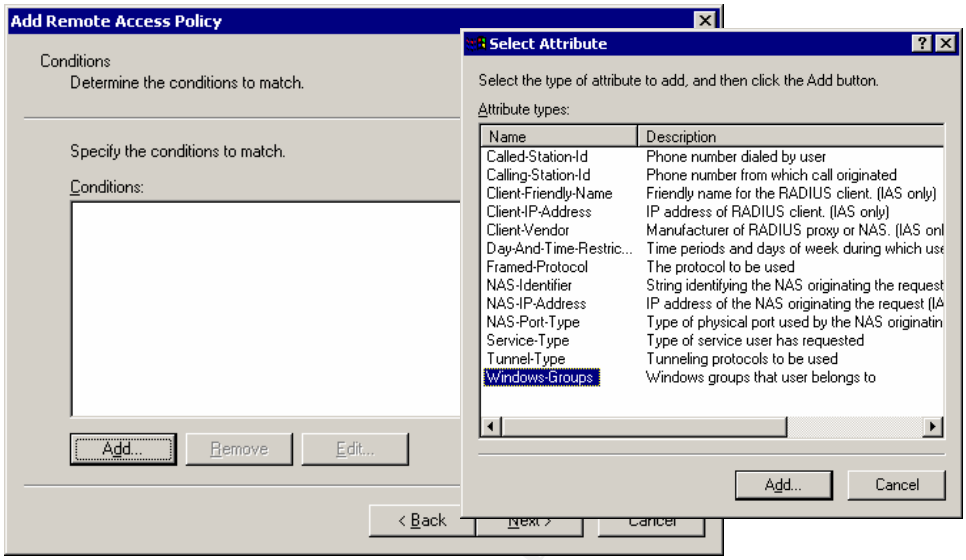


SETTING UP THE EXEC MODE ACCESS POLICY FOR CISCO ADMINISTRATORS

4. Right-click on the Remote Access Policies container in the left pane of the MMC and select New Remote Access Policy. Enter a descriptive name for the policy:

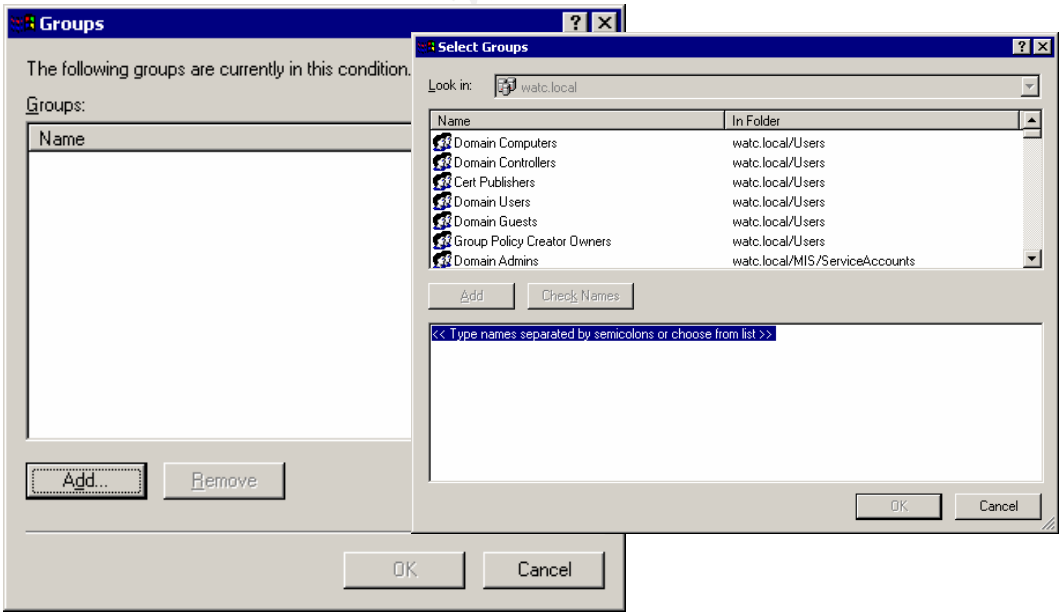


5. Select Add to add a condition for authorization and select from the available options. Generally, you will use Windows Groups for AD based rules:

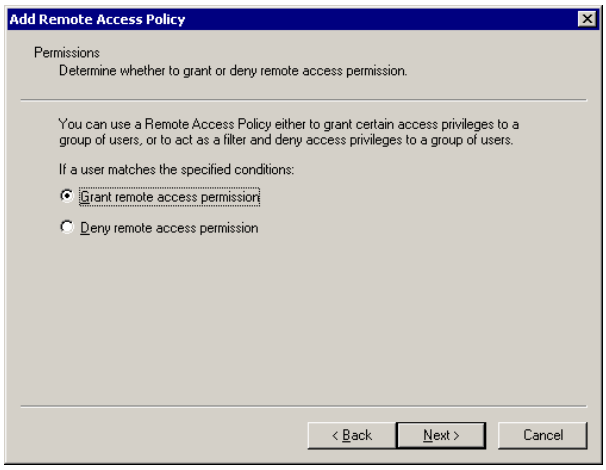


Note: When using a combination of attributes, all specified conditions must be evaluated true for the remote access policy to be applied.

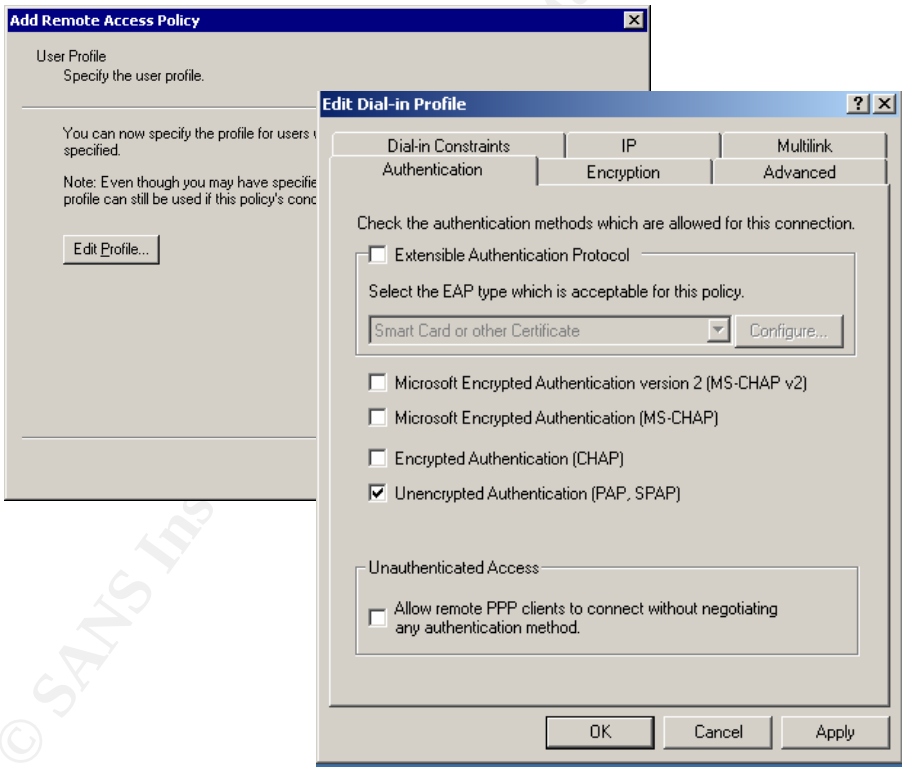
6. Click add to add a group and select the group from AD you want to use for authorization:



7. Select Grant for the permission:

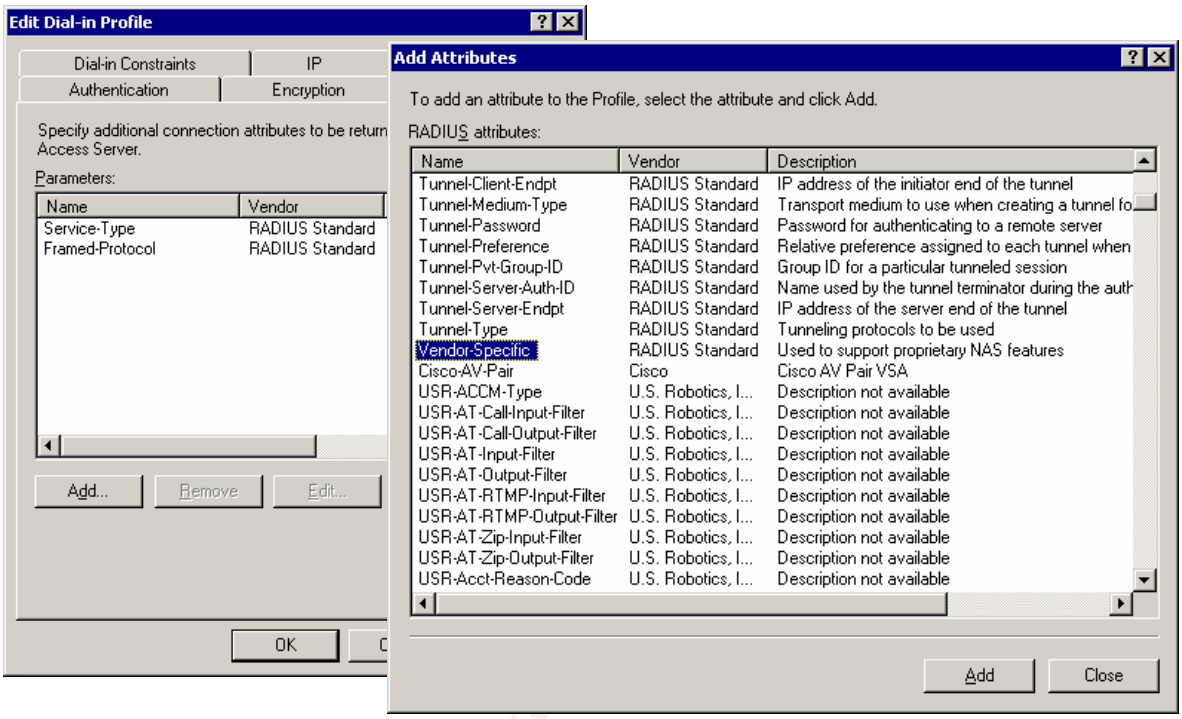


8. Click the “Edit Profile” button and Select the Authentication tab and enable PAP authentication. CHAP, MS-CHAP and MS-CHAP v2 are not supported for this implementation.

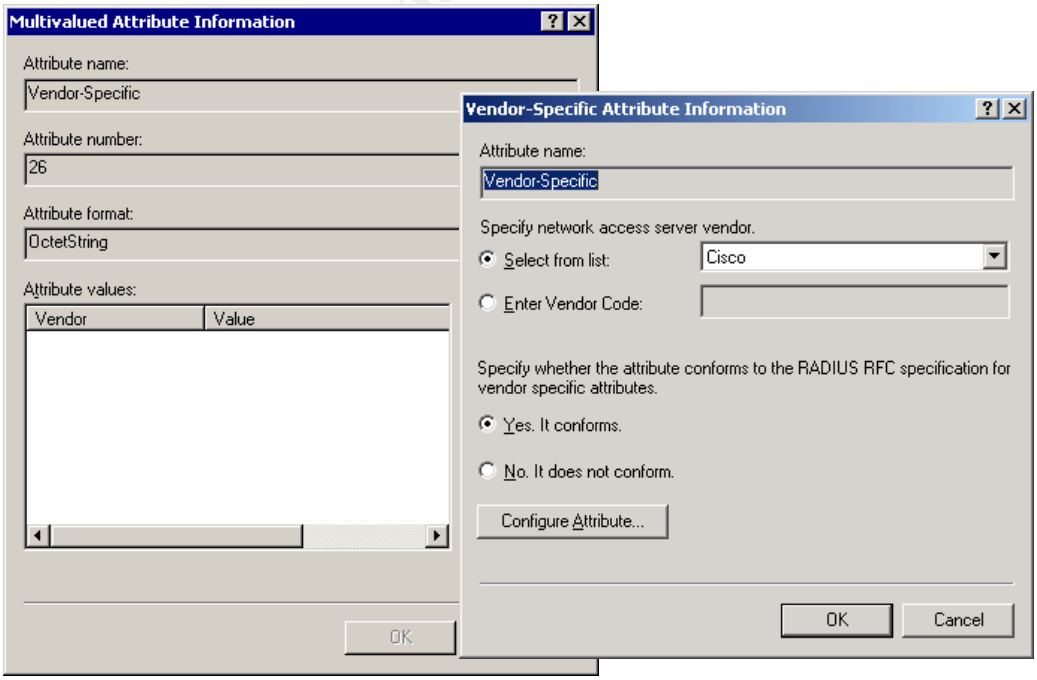


Note: Password Authentication Protocol (PAP) does not natively provide password or username encryption during the authentication process. However, Cisco IOS will use the shared secret identified in the previous step to encrypt the password. The username will be sent in the clear. Therefore, the use of a short shared secret will not provide as strong a level of password encryption.

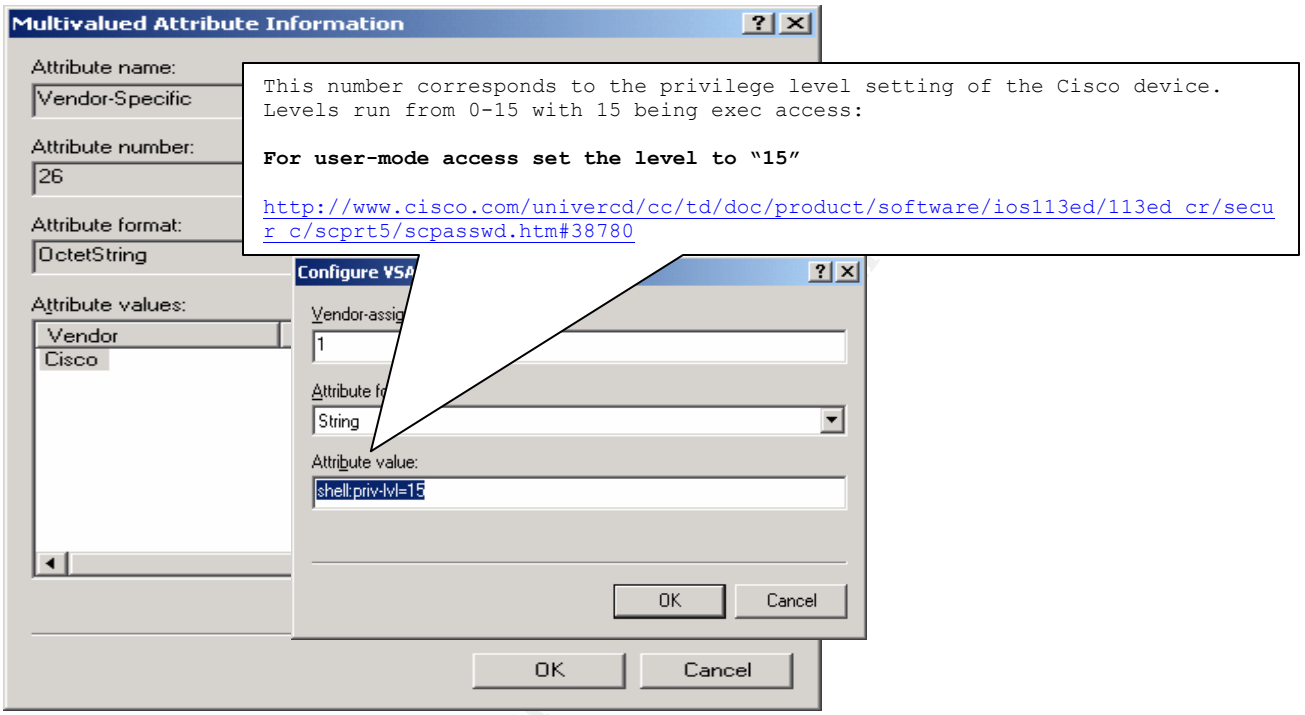
9. On the Advanced tab select add to add a vendors specific option:



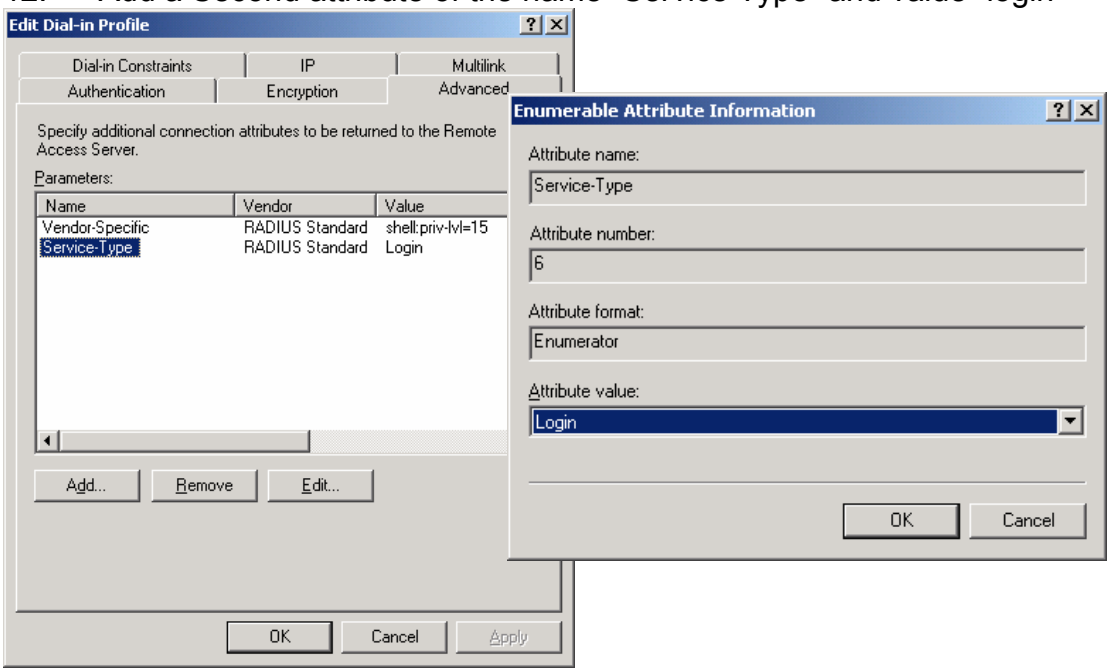
10. Click on “add” to add an attribute and make the following selections.



11. Select Configure Attribute and enter the following in the Attribute Value Box: “Shell:priv-lvl=15”



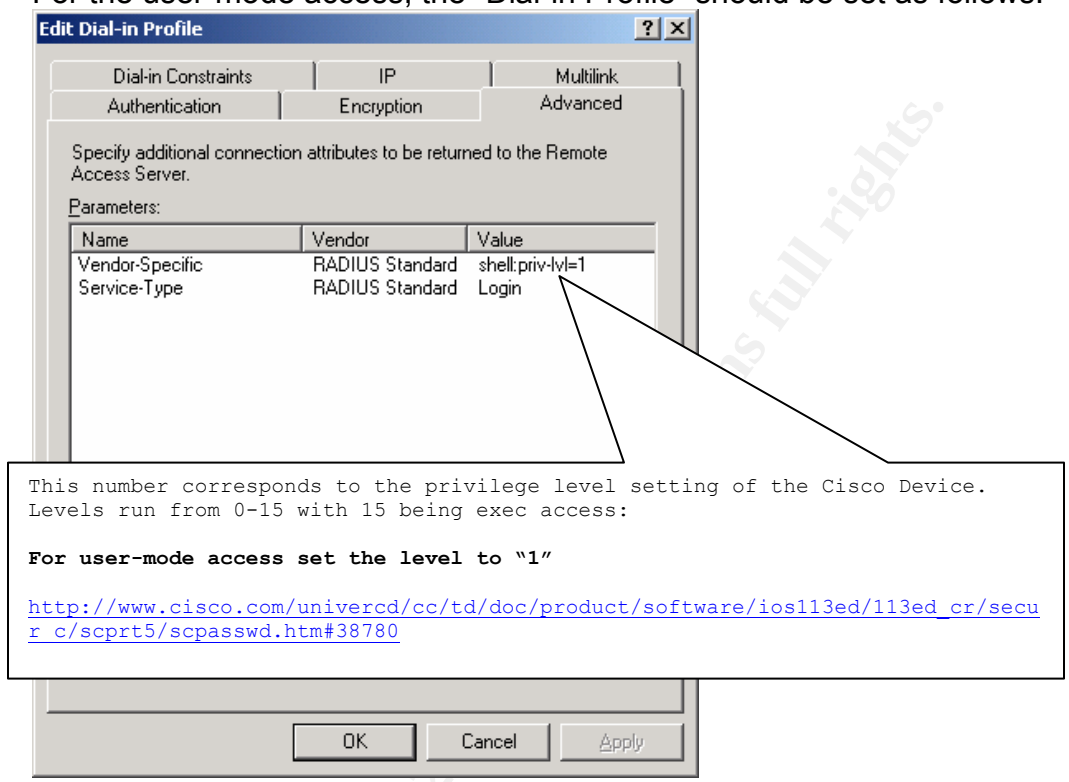
12. Add a Second attribute of the name “Service Type” and value “login”



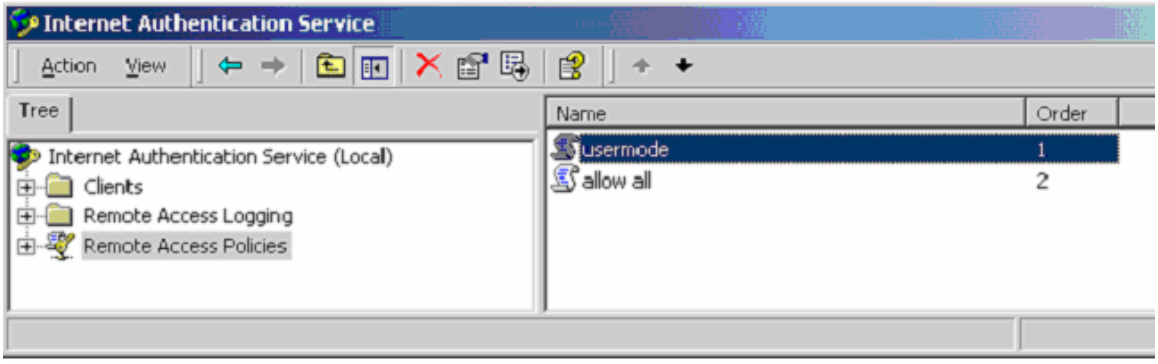
Create another rule for "user-mode" access to the Cisco device

13. Repeat steps 8 – 13 this time naming the rule to reflect the lower level of access that will be granted.

For the user-mode access, the "Dial-in Profile" should be set as follows:



14. You will now see the rule you created in the MMC. It is important to remember that the rules will be applied in order. Once the RADIUS (IAS) server finds a match it will stop processing the remaining rules. THE ORDER IS IMPORTANT.



The key to the process that IAS uses to authenticate users is that it analyzes the RADIUS request against the available rules sequentially. The processing of these rules only continues until a match is found. This

becomes relevant in two examples for authorizing Cisco administrators. Because we are evaluating the “usermode” rules first if a Cisco administrator is in both the CiscoAdmins and CiscoReadOnly groups they will never be granted any more than usermode access. Additionally, if a request would match a deny prior to a grant rule or vice versa users could be granted or denied access in an unintended manor. If you want a deny access rule to override an allow rule it is important that the deny rules is placed earlier in the order.

SETTING UP THE CISCO CONFIGURATION (SWITCHES AND ROUTERS)

1. The AAA command is used to configure authorization in the Cisco IOS. You will need to enter the following commands to Setup a new authentication model and specify several authentication groups for exec mode, local login and default.

```
aaa new-model
aaa authentication login default group radius
aaa authentication login if_needed local
aaa authorization exec default group radius if-authenticated
```

   The purpose of the default login and exec group is to force the router or switch to use RADIUS as its default method for authenticating users. The “if_needed” group referencing local is used to allow a local database username and password for console access if the IAS server is unavailable. Obviously it is important to provide a secondary form of authentication if the network or IAS server cannot be contacted by the Cisco equipment

2. Setup the RADIUS server configuration on the equipment.

```
radius-server host 192.168.0.185 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key SharedSecret
```

3. Change the default privilege level at which the enable command becomes available:

```
privilege exec level 2 enable
```

   Privilege levels on Cisco equipment range from 1 to 15 with 15 representing full exec capabilities. Level 15 is the default level for enable mode on a Cisco device. By default the enable command which will prompt a user for a password to enter exec mode is available at all privilege levels. By setting the level at which that command becomes available to 2 we can prevent users from attempting password guessing or brut force attacks against the enable password.

4. Create the local user and password for console access. The following commands are entered under the "`line con 0`" configuration.

```
username cisco password CiscoPassword
privilege level 2
login authentication if_needed
```

Note: Complete configuration files for a router and IOS based Catalyst switch have been placed in the appendix A and B.

DYNAMICALLY ASSIGNING FIREWALL RULES WITH IAS

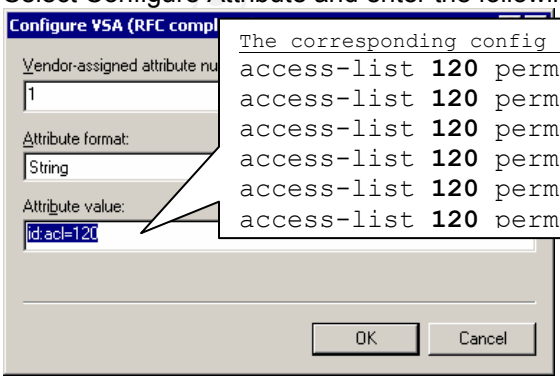
The same concepts that where employed to allow network administrators and engineers to connect to and manage Cisco switches and routers can be used to dynamically assign firewall rulesets based on a users Active Directory group membership. This section describes how to use a IAS server to grant users access through a pix firewalls by dynamically assigning Access Control Lists (ACL's) to users based on Active Directory Group Membership.

CONFIGURING THE IAS SERVER

Follow the same steps outlined for the setup of RADIUS server for logon AAA services:

1. Setup a Client for the PIX firewall in the IAS management console.
2. Following all the same steps that where used to setup the IAS server for switch or router authentication, configure the IAS server to support requests from the pix firewall. When configuring the "vendor specific" attributes on the remote access policy profile, use the "id:acl=<acl>" syntax to assign a PIX ACL group to the remote access policy.

Select Configure Attribute and enter the following information:



The corresponding config on the PIX (**number** must match on both sides)

```
access-list 120 permit tcp any host 10.1.1.10 eq www
access-list 120 permit tcp any host 10.1.1.10 eq 443
access-list 120 permit tcp any host 10.1.1.11 eq 443
access-list 120 permit tcp any host 10.1.1.12 eq 443
access-list 120 permit tcp any host 10.1.2.10 eq 443
access-list 120 permit tcp any host 10.1.2.10 eq www
```

Note: this configuration will apply access list number 120 to any user matching the remote access policy defined on the IAS server.

CONFIGURING THE PIX FIREWALL

The steps for configuring the PIX firewall are extremely straight forward. The access-list commands are used to assign the appropriate rules set to users based on the "vendor specific attribute" returned by the IAS server during the authentication process.

1. Configure the access lists to allow the desired traffic for the users granted access by the remote access policy on the IAS server:

```
access-list 120 permit tcp any host 10.1.1.10 eq www
access-list 120 permit tcp any host 10.1.1.10 eq 443
access-list 120 permit tcp any host 10.1.1.11 eq 443
access-list 120 permit tcp any host 10.1.1.12 eq 443
access-list 120 permit tcp any host 10.1.2.10 eq 443
access-list 120 permit tcp any host 10.1.2.10 eq www
```

   In this example, users assigned access list "120" will be allowed to communicate via http to 10.1.1.10 and 10.1.2.10 and via SSL to 10.1.1.10-12 and 10.1.2.10.

2. Once the access list has been setup the following command is used to force specific types of traffic to be authorized via RADIUS:

```
access-list radius permit ip any any
```

   The above command would force all traffic to be authenticated via RADIUS. In order to allow certain traffic to pass without being authenticated by RADIUS the following access list can be used to exclude traffic from requiring RADIUS authentication:

```
access-list radius deny tcp any host 10.1.3.23 eq smtp
```

   The above command would allow any incoming mail traffic to pass to our mail server without RADIUS authentication.

3. The next step in the process is to configure the RADIUS server to be used by the PIX:

```
aaa-server AuthInbound protocol radius
aaa-server AuthInbound (inside) host 10.1.3.20 SharedSecret
aaa authentication match radius outside SharedSecret
```

   In the above example, the first line defines an authentication group called "AuthInBound". The second line defines the location of our IAS server. In this case, the IAS server is found in the "inside" interface of our firewall at an address of 10.1.3.20 and is connected to using the shared secret "SharedSecret". The final command is used to specify the traffic that will be authenticated via our IAS server. In this example, any traffic matching the

criteria in the access-list named “radius” will require authorization by our IAS server.

Note: An important note is that the “outside” parameter in the last line results in this authentication only be required by traffic originating on the “outside” interface. This example does not effect normal outbound traffic.

4. Set the timeouts for RADIUS authenticated sessions with the “`timeout uauth hh:mm:ss`” command:

```
timeout uauth 0:30:00 absolute uauth 0:25:00 inactivity
```

The above command results in sessions being timed out after 30 minutes regardless of activity or after 25 minutes of inactivity.

RECOMMENDATIONS

REMOTE ACCESS POLICY ORDER

As with assigning multiple levels of administrative access to Cisco equipment via IAS, the rules for assigning an access-list on a PIX firewall are evaluated sequentially. This will result in the first match being utilized and will make the order of your policies on the IAS server extremely important. The result of this implementation is the need for a separate “remote access policy” for each combination of remote access policies. All of these separate policies will need to correspond of a unique access-list on the PIX firewall. There is not an ability to apply multiple access policies or nest the policies. This can be important in the implementation depending on the complexity of the access policies required.

APPLICATION SUPPORT OF RADIUS

Many applications natively support RADIUS authentication. When connecting though a pix firewall configured with IAS as described with one of these applications the users will be prompted to enter there windows username and password by the firewall once the RADIUS authorization is required. This is the case with Microsoft Internet Explorer and Netscape Navigator browsers for HTTP traffic. However, users attempting to communicate on HTTPS will not be authenticated. The result in this implementation would be that users would need to be directed to a standard HTTP page to initiate the RADIUS/IAS prompt and then, after being authenticated by the firewall, would be free to navigate to the https based web pages or anything else allowed by the access-list applied.

Note: In this example, users have an absolute timeout of 30 minutes and exceed this connection time they will be required to navigate back to the original HTTP page to get another RADIUS authentication prompt.

AUDITING THE IAS SERVER

Once the IAS server is operating to provide authentication and authorization services for your Cisco infrastructure, it will be important to provide reporting and auditing capabilities of this service. The information will be contained in the application event log on the IAS server or the text based logfiles created by the IAS service.

WINDOWS 2000 IAS LOG FILES

By default windows IAS server writes a text based log files to the \winnt\system32\logfiles directory. The default filename is iaslog.log. By default there is no logging enabled in the IAS server. To enable logging, navigate to the properties of the "local file" under the "Remote Access Logging" section of the IAS management console. Under the settings tab of the properties setup logging of "Accounting Requests", "Authentication requests" and "periodic status updates". In most cases all options should be enabled.

IAS FORMATTED LOG FILES

You can set up your IAS servers to log the data using either the database-import log format or IAS format. If you select the IAS format, attributes are logged in the form of attribute-value pairs. This format has the following characteristics:

- The sequence of the attributes is dependent on the RADIUS client sending a request.
- The logged attributes include RADIUS-standard, IAS-specific, and vendor-specific attributes.
- All attributes containing unprintable characters or any delimiter (such as | or ,) will be printed in hexadecimal format (for example, 0x026).

DATABASE FORMATTED LOG FILES

If you select the database-import log format, attributes are logged in a format that supports importing the log into databases. This format has the following characteristics:

- The attributes of all records are recorded in the same sequence (pre-defined by IAS), regardless of which client sent the request. This sequence includes a set specific set of attributes and, although limited in number, are the attributes that are generally most useful for tracking and analysis of requests.
- If the attribute is not present in the request or reply, then the field is empty in the log.
- A specific set of attributes is logged in a sequence that is pre-defined in IAS. The attributes included in this set are pre-defined in IAS and, although limited in number, are those that generally are the most useful for tracking and analysis of requests.

Database-import log file formats are recommended for most environments because you can then more easily import the log files into databases. The consistent structure of this format facilitates the tracking and analysis of the data. To collect the data directly into another process, you can configure IAS to write a named pipe, in the instead of a file. To use named pipes, set the log file folder to \\.\pipe or \\computername\pipe. The named pipe server program should create a named pipe called \\.\pipe\iaslog.log to accept the data.

Log Rotation

By default, log files will grow to an unlimited file size. This setting can be changed to start a new log file after the current files reaches a specific file size or on a timed basis (monthly, daily or weekly). For consistency it is generally recommended that files are created based on time (i.e. daily, monthly or weekly) rather than file size.

Windows 2000 Event Logs

Some information that will not be included in IAS log files but will be collected in the application log includes service errors and status messages. In relation to user authentication logging, the settings that are selected in the "Remote Access Logging" section of the IAS server configuration for log file configuration are enforced for event log reporting as well.

Best Practices and Recommendations

Network Time Protocol

In order to ensure that logging on both the Cisco devices and the IAS server are synchronized, it is important to ensure that the Cisco devices are utilizing the same time source as the Windows 2000 environment. By default, member servers in an active directory domain will synchronize to the domain time. Cisco devices will need to be configured with the following command:

```
ntp peer ip-address [version number] [key keyid]
[source interface] [prefer]
```

Shared Secret

An important weakness in the authentication of RADIUS clients to RADIUS server is the static nature of the shared secret. A basic recommendation is to maintain uniqueness of these shared secrets for all devices. Although this can create significantly greater management burdens, it forces an attacker to obtain the password for each device on behalf of which they where attempting to authenticate.

PROVIDING FAULT TOLERANCE WITH IAS

After configuring Cisco devices to require RADIUS authentication, the availability of the IAS server to provide that authentication is important. Two primary methods can be used to provide basic redundancy for IAS. The first, is the configuration of two IAS servers utilizing Windows Network Load Balancing to provide both failover and load balancing for IAS services. The second is to configure multiple RADIUS servers in the Cisco devices using timeouts values to specify the amount of time the Cisco device will wait before requesting the authentication from the secondary RADIUS server.

RECOVERY PROCESS FOR IAS

Providing recovery capability for you IAS infrastructure can be important. In order to do a manual backup of the IAS configuration including registry settings, execute the following command:

```
C:>netsh aaaa show config <path>\file.txt
```

This command stores the entire IAS configuration into the text file. To restore the configuration to the same IAS server or a different IAS server execute the following command:

```
C:>netsh exec <path>\file.txt
```

A message indicating whether the import was successful will be displayed after executing the command.

CONFIGURING RADIUS PORT SETUP

By default, RADIUS, and likewise IAS, use UDP port 1645 and 1812 for RADIUS authorization processes and UDP port 1646 and 1813 for accounting functions. Because of the well-known nature of these port assignments it could be beneficial to configure your IAS server to listen for RADIUS requests on alternative ports. To do this:

1. Open IAS
2. Right-Click on the IAS Server and then select Properties.
3. On the RADIUS tab, set the port numbers to the desired setting.

You can use multiple ports for the authentication or accounting functions by separating them with commas (i.e. 1813,1646,3342, etc). The critical concept to remember is that your RADIUS clients (Cisco devices) must be set to communicate to the IAS server on the same port(s). This can be changed on the Cisco switch or router with the following configuration:

```
radius-server host 192.168.0.185 auth-port <port> acct-port <port>
```

MANAGING WINDOWS GROUPS AND CISCO ACCESS

Because the Remote access policies are evaluated in sequential order with the first match resulting the application of that policy the structure of your groups and policies are important. A general design approach that is employed in this guide is to create windows groups such as CiscoAdmins, CiscoLevel2, CiscoLevel3, etc. Once these groups have been created, users can be placed in the highest level group, in terms of access.

ACCOUNT LOCKOUT

Although you might have implemented account lockout policies for failed logon attempts to Windows via a Group Policy Object, those policies will not be enforced inherently with IAS. In order to implement a lockout policy for IAS logon attempts, the registry must be edited on the IAS server. Locate the following key:

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Remote Access\Parameters\AccountLockout

Under that key, the following values are required to be edited:

> **MaxDenials:** The default is set at 0 and represents the number of failed attempts before the account is denied access.
>
> **ResetTime:** The default value is set at 0xb40, or 2,880 minutes (48 hours). This value should be changed to reflect the number of minutes before the failed attempts counter is reset.

To manually reset an account that has been locked out before the failed attempts counter is automatically reset, delete the following registry subkey that corresponds to the user's account name:

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Remote Access\Parameters\AccountLockout\domain name:user name

CONCLUSION – SUMMARY

Utilizing IAS to provide centralized AAA services for your Cisco infrastructure can be an extremely effective way to manage access. Many organizations already have Active Directory accounts setup for network administrators. The ability to consolidate the management of access without the additional cost of a third-party RADIUS solution can provide a significant benefit to many organizations.

REFERENCES

Request For Comments 2138. Ed. Livingston, Rubens, Merit, Daydreamer, Willens Livingston. Apr. 1997. < http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2138.html#sec-2>

Internet Authentication Service for Windows 2000. <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/ias.asp >

Cisco IOS Technologies: RADIUS Support in Cisco IOS Software. <http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iolk/tech/rdius_wp.pdf>

Configuring RADIUS, Cisco Systems <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt2/scdrad.htm>

Configuring Passwords and Privileges, Cisco Systems. <http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt5/scpasswd.htm#38780>

Controlling Switch Access with RADIUS, Cisco Systems <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12111ea1/scg/swadmin.htm#xtocid22>

Release Notes for the Catalyst 2900 XL and Catalyst 3500 XL Switches, Cisco IOS Release 12.0(5)WC5 Switch Requirements http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc5/ol256201.htm#xtocid17

APPENDIX A: ROUTER CONFIGURATION

Sample configuration:	Comments
version 12.2	
service timestamps debug uptime	
service timestamps log uptime	
!	
hostname labrouter	
!	
aaa new-model	Establish an AAA model
aaa authentication login default group radius	Set the default auth type to radius
aaa authentication login if_needed local	user database for console access
aaa authorization exec default group radius if-authenticated	Set the exec-mode to use radius
enable secret enablepassword	
!	
username cisco password CiscoPassword	Setup a local username
ip subnet-zero	
!	
ip domain-name router.wichitatech.com	
!	
ip audit notify log	
ip audit po max-events 100	
ip ssh time-out 60	
ip ssh authentication-retries 2	
!	
call rsvp-sync	
!	
interface FastEthernet0/0	
no ip address	
speed 100	
full-duplex	
!	
interface Ethernet1/0	
ip address 172.16.0.253 255.255.255.0	
full-duplex	
!	
ip classless	
ip route 0.0.0.0 0.0.0.0 172.16.0.254	
no ip http server	Set location of the RADIUS server
ip pim bidir-enable	
!	
radius-server host 192.168.0.185 auth-port 1645 acct-port 1646	
radius-server retransmit 3	Establish the key. (this matches the key on the RADIUS (IAS) server.
radius-server key SharedSecret	
!	
dial-peer cor custom	Move the exec command to priv level 2 so that users authenticating as part of the user-mode group cannot enter enable mode.
!	
privilege exec level 2 enable	
!	
!	
!	
!	Set console access to go to level 2
line con 0	
privilege level 2	
logging synchronous	Set console access to use local user database
login authentication if_needed	
line aux 0	
line vty 0 4	
password 7 040958360E2A785B054C	
logging synchronous	
!	
end	

APPENDIX B: SWITCH CONFIGURATION

Sample configuration:	Comments
version 12.0	
no service pad	
service timestamps debug uptime	
service timestamps log uptime	
no service password-encryption	
!	
hostname labswitch	
!	
aaa new-model	Establish an AAA model
aaa authentication login default group radius	Set the default auth type to radius
aaa authentication login if_needed local	user database for console access
aaa authorization exec default group radius	Set the exec-mode to use radius
enable secret 5 CiscoPassword	
enable password CiscoPassword	
!	
username cisco password 0 cisco	Setup a local username
!	
ip subnet-zero	
ip domain-name lab.com	
!	
[PORT CONFIGURATION OMMITED]	
!	
interface VLAN1	
ip address 192.168.200.1 255.255.255.0	
no ip directed-broadcast	
no ip route-cache	
!	
ip default-gateway 192.168.200.20	
radius-server host 192.168.0.185 auth-port 1645	Set location of the RADIUS server
acct-port 1646	
radius-server key cisco	Establish the key. (this matches the key on the RADIUS (IAS) server.
!	
privilege exec level 2 enable	Move the exec command to priv level 2 so that users authenticating as part of the user-mode group cannot enter enable mode.
!	
!	
!	
!	
!	
line con 0	
privilege level 2	Set console access to go to level 2
login authentication if_needed	Set console access to use local user database
transport input none	
stopbits 1	
line vty 0 4	
password CiscoPassword	
line vty 5 15	
!	
end	