

PIX/ASA: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example

Document ID: 91831

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions
- Network Diagram

Background Information

Configure

- Configure the Security Appliance
- Configure the LDAP Server

Verify

- View Sessions

Troubleshoot

- LDAP Debugging
- Attributes Not Mapped

Related Information

Introduction

This document provides a sample configuration for SSL VPN clients (SVC) that connect to Cisco 5500 Series Adaptive Security Appliance (ASA) and then get mapped to different VPN group policies based on a response from a Microsoft Lightweight Directory Access Protocol (LDAP) server. The ASA 7.2.2 software provides LDAP attribute mapping, which allows attributes that are sent from the LDAP server to be mapped to attributes recognized by the ASA, such as IETF RADIUS attribute 25 (Class).

In this example, users who are allowed dial-in access in the AD/LDAP server are mapped to the `ALLOWACCESS` group policy, and the users who are not allowed dial-in access are assigned to the `NOACCESS` group policy on the ASA. The `NOACCESS` group policy has the number of allowed VPN sessions set to 0, which causes the user connection to fail.

Note: This configuration uses the SSL VPN client, but the same principles can be applied to group policies used for other VPN clients. Moreover, this configuration can be used for purposes other than to deny VPN access. In this example, LDAP attributes are simply used to map a group policy to a user. The details of that policy (such as allowed protocols, split tunnel list, or VPN filter) can be configured as desired.

Note: WebVPN features, such as the SVC are only available on the ASA 5500 Series Security Appliance, not the PIX 500 Series.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- You are familiar with SVC (SSL VPN client) configuration in ASA.
- You are familiar with LDAP configuration on your server.

Refer to RFC 3377 to learn more about the LDAP protocol.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance (ASA), which runs software version 7.2.2
- Cisco SSL VPN Client 1.1.3.173
- Microsoft Windows 2003 Enterprise Server with Service Pack 1 (SP1)

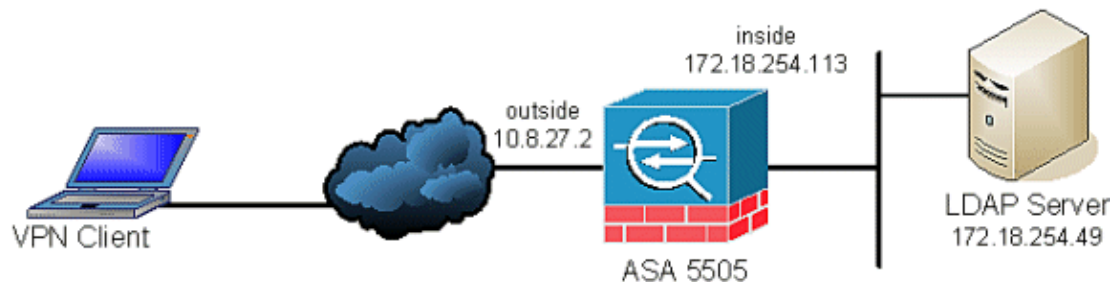
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses that have been used in a lab environment.

Background Information

In this example, the AD/LDAP attribute `msNPAllowDialin` is mapped to the ASA attribute `CVPN3000-Radius-IETF-Class`. The class attribute is used to enforce group policies on the ASA.

1. The user initiates a SVC connection to the ASA.
2. The ASA is configured to authenticate SVC users with the Microsoft AD/LDAP server.
3. The ASA binds to the LDAP server with the credentials configured on the ASA (Administrator in this case) and looks up the provided username.
4. If the username is found, the ASA attempts to bind to the LDAP server with the credentials that the user provided at login.
5. If the second bind is successful, the ASA retrieves the users attributes, which includes **msNPAllowDialin**.
6. The **msNPAllowDialin** attribute is mapped to **CVPN3000-Radius-IETF-Class** by the configured LDAP attribute map.

- ◆ The FALSE value is mapped to NOACCESS
 - ◆ The TRUE value is mapped to ALLOWACCESS
7. The **CVPN3000–Radius–IETF–Class** attribute is examined and a group policy determination is made.
- ◆ The NOACCESS value causes the NOACCESS group policy to be assigned to the user.
 - ◆ The ALLOWACCESS value causes the ALLOWACCESS group policy to be assigned to the user.
8. If the NOACCESS policy is applied, the users sees the login fail. If the ALLOWACCESS policy is applied, the connection proceeds normally.

Configure

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Configure the Security Appliance

ASA configuration:

Cisco ASA
<pre> CiscoASA #show running-config : Saved : ASA Version 7.2(2) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Vlan1 nameif inside security-level 100 ip address dhcp ! interface Vlan2 nameif outside security-level 0 ip address 10.8.27.2 255.255.255.0 ! interface Ethernet0/0 ! interface Ethernet0/1 shutdown ! interface Ethernet0/2 shutdown ! interface Ethernet0/3 shutdown ! interface Ethernet0/4 shutdown ! interface Ethernet0/5 switchport access vlan 2 ! interface Ethernet0/6 shutdown </pre>

```
!  
interface Ethernet0/7  
  shutdown  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
boot system disk0:/asa722-k8.bin  
ftp mode passive  
dns server-group DefaultDNS  
  domain-name default.domain.invalid  
  
!--- Access list to exempt traffic to the VPN clients from NAT  
  
access-list NONAT extended permit ip any 192.168.100.0 255.255.255.0  
  
pager lines 24  
mtu inside 1500  
mtu outside 1500  
  
!--- IP address pool for the VPN clients  
  
ip local pool CISCOPOOL 192.168.100.1-192.168.100.254  
  
no failover  
icmp unreachable rate-limit 1 burst-size 1  
asdm image disk0:/asdm-522.bin  
no asdm history enable  
arp timeout 14400  
  
!--- NAT configuration  
  
global (outside) 1 interface  
nat (inside) 0 access-list NONAT  
nat (inside) 1 0.0.0.0 0.0.0.0  
  
route outside 0.0.0.0 0.0.0.0 10.8.27.1 1  
timeout xlate 3:00:00  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00  
timeout uauth 0:05:00 absolute  
  
!--- The LDAP attribute map. msNPAllowDialin is  
  mapped to cVPN3000-IETF-Radius-Class  
!--- A value of FALSE is mapped to a value of NOACCESS  
!--- A value of TRUE is mapped to a value of ALLOWACCESS  
  
ldap attribute-map CISCOMAP  
  map-name msNPAllowDialin cVPN3000-IETF-Radius-Class  
  map-value msNPAllowDialin FALSE NOACCESS  
  map-value msNPAllowDialin TRUE ALLOWACCESS  
  
!--- AAA server configuration  
  
aaa-server LDAPGROUP protocol ldap  
aaa-server LDAPGROUP host 172.18.254.49  
  ldap-base-dn dc=rtpsecurity, dc=cisco, dc=com  
  ldap-scope subtree  
  ldap-naming-attribute sAMAccountName  
  ldap-login-password *  
  ldap-login-dn CN=Administrator,CN=Users,DC=rtpsecurity,DC=cisco,DC=com  
  server-type microsoft
```

```
ldap-attribute-map CISCOMAP
```

```
!--- The NOACCESS group policy.  
!--- vpn-simultaneous-logins is 0 to prevent access
```

```
group-policy NOACCESS internal  
group-policy NOACCESS attributes  
vpn-simultaneous-logins 0  
vpn-tunnel-protocol IPSec webvpn  
webvpn  
svc required
```

```
!--- The ALLOWACCESS group policy
```

```
group-policy ALLOWACCESS internal  
group-policy ALLOWACCESS attributes  
banner value This is the ALLOWACCESS Policy  
vpn-tunnel-protocol IPSec webvpn  
webvpn  
svc required
```

```
username cisco password ffIRPGpDSOJh9YLq encrypted  
no snmp-server location  
no snmp-server contact  
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
!--- The tunnel group that users connect to
```

```
tunnel-group TESTWEBVPN type webvpn  
tunnel-group TESTWEBVPN general-attributes  
address-pool CISCOPOOL  
authentication-server-group LDAPGROUP  
tunnel-group TESTWEBVPN webvpn-attributes  
group-alias TestWebVPN enable
```

```
telnet timeout 5  
ssh timeout 5  
console timeout 0
```

```
!  
class-map inspection_default  
match default-inspection-traffic  
!  
!  
policy-map type inspect dns preset_dns_map  
parameters  
message-length maximum 512  
policy-map global_policy  
class inspection_default  
inspect dns preset_dns_map  
inspect ftp  
inspect h323 h225  
inspect h323 ras  
inspect netbios  
inspect rsh  
inspect rtsp  
inspect skinny  
inspect esmtp  
inspect sqlnet  
inspect sunrpc
```

```

inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global

!--- The WebVPN configuration. "tunnel-group-list enable"
!--- allows users to choose the TESTWEBVPN tunnel group at login.

webvpn
enable outside
svc image disk0:/sslclient-win-1.1.3.173.pkg 1
svc enable
tunnel-group-list enable

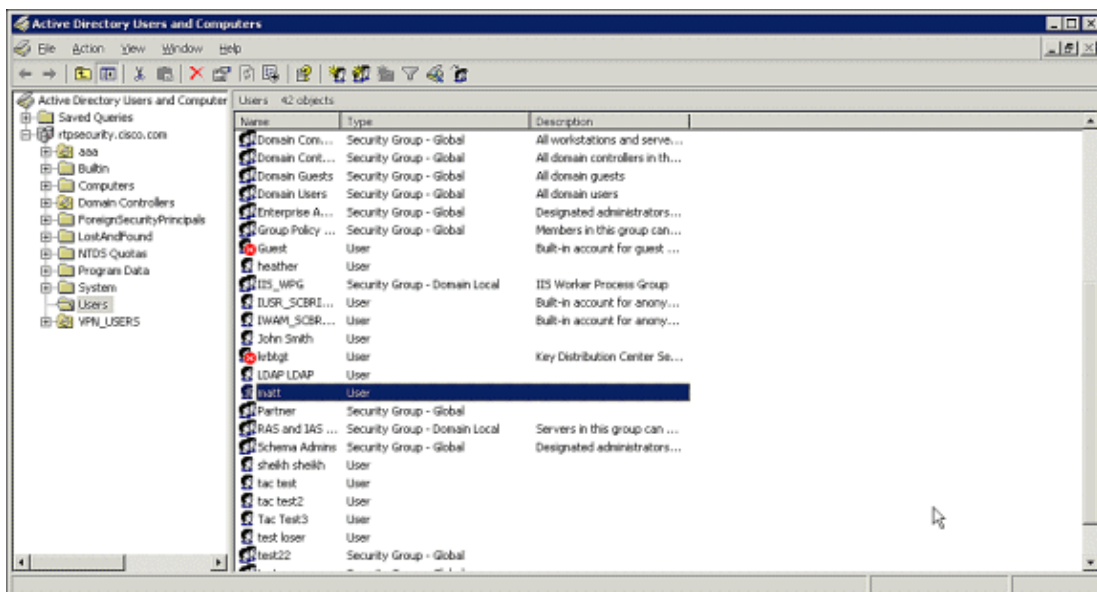
prompt hostname context
Cryptochecksum:80879cf44975e65beed984ee308f7c57
: end

```

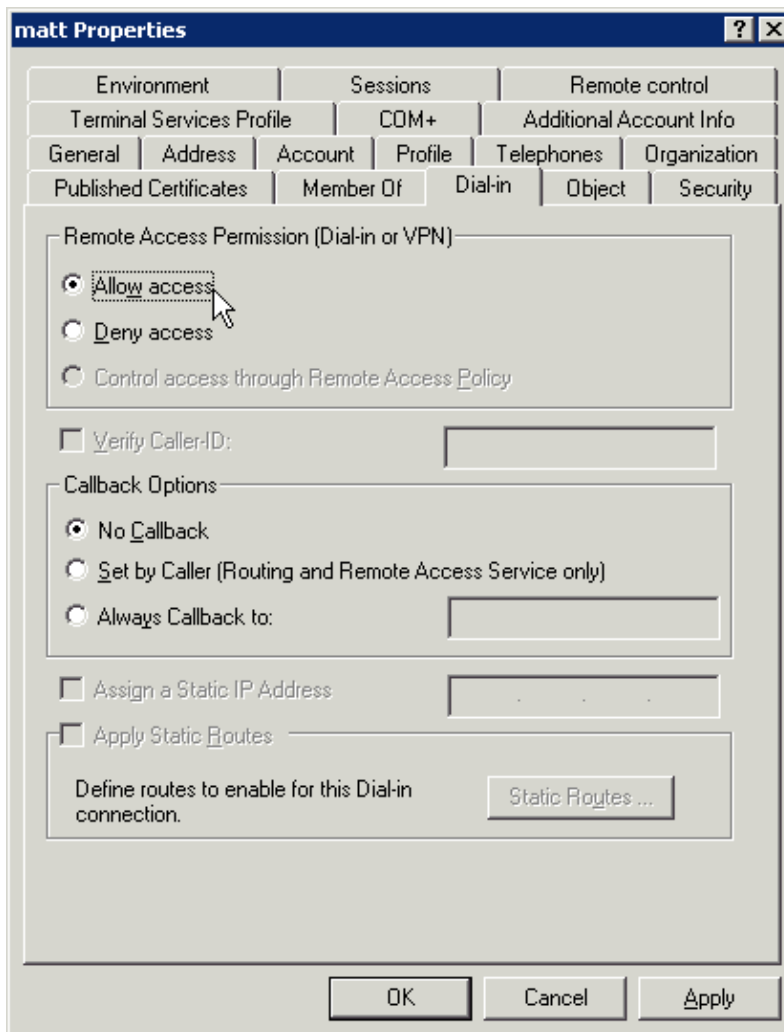
Configure the LDAP Server

Complete these steps to configure the LDAP Server:

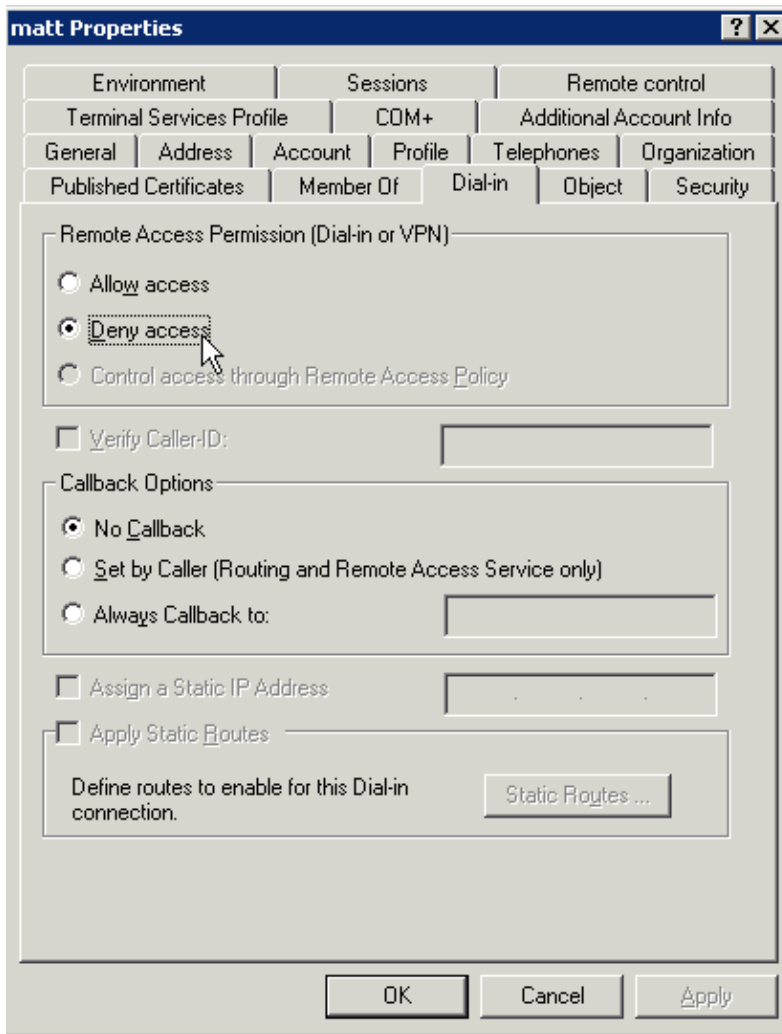
1. Choose a user in the Active Directory.



2. Configure the user to allow or deny dial-in access.



OR



Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

View Sessions

Use the **show vpn-sessiondb detail svc** command to see the connected SVC sessions. In the below example, the user **matt** has been assigned the **ALLOWACCESS** policy as expected.

```
ciscoasa# sh vpn-sessiondb detail svc

Session Type: SVC Detailed

Username      : matt
Index         : 1
Assigned IP   : 192.168.100.1      Public IP    : 10.8.27.10
Protocol      : SVC                Encryption   : 3DES
Hashing       : SHA1              Auth Mode    : userPassword
TCP Dst Port  : 443                TCP Src Port : 1393
Bytes Tx      : 130163             Bytes Rx     : 2625
Pkts Tx       : 131                Pkts Rx     : 13
Pkts Tx Drop  : 0                  Pkts Rx Drop : 0
Client Type   : Mozilla/4.0 (compatible; MSIE 6.0;
```

```
Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 3, 173
Group Policy : ALLOWACCESS
Tunnel Group : TESTWEBVPN
Login Time   : 16:15:03 UTC Thu Aug 9 2007
Duration     : 0h:00m:05s
Filter Name  :
```

Troubleshoot

LDAP Debugging

When LDAP debugging is enabled, you can see the attribute mapping process. The first example shows the entire output when **msNPAllowDialin** is set to TRUE. The second example shows the relevant output when the value is FALSE.

msNPAllowDialin is TRUE:

```
ciscoasa# debug ldap 255
debug ldap enabled at level 255
ciscoasa#
[34] Session Start
[34] New request Session, context 0x3bbe9f4, reqType = 1
[34] Fiber started
[34] Creating LDAP context with uri=ldap://172.18.254.49:389
[34] Binding as administrator
[34] Performing Simple authentication for Administrator to 172.18.254.49
[34] Connect to LDAP server: ldap://172.18.254.49:389, status = Successful
[34] LDAP Search:
      Base DN = [dc=rtpsecurity, dc=cisco, dc=com]
      Filter  = [sAMAccountName=matt]
      Scope   = [SUBTREE]
[34] User DN = [CN=matt,CN=Users,DC=rtpsecurity,DC=cisco,DC=com]
[34] Talking to Active Directory server 172.18.254.49
[34] Reading password policy for matt,
      dn:CN=matt,CN=Users,DC=rtpsecurity,DC=cisco,DC=com
[34] Read bad password count 0
[34] Binding as user
[34] Performing Simple authentication for matt to 172.18.254.49
[34] Checking password policy for user matt
[34] Binding as administrator
[34] Performing Simple authentication for Administrator to 172.18.254.49
[34] Authentication successful for matt to 172.18.254.49
[34] Retrieving user attributes from server 172.18.254.49
[34] Retrieved Attributes:
[34]   objectClass: value = top
[34]   objectClass: value = person
[34]   objectClass: value = organizationalPerson
[34]   objectClass: value = user
[34]   cn: value = matt
[34]   givenName: value = matt
[34]   distinguishedName: value = CN=matt,
      CN=Users,DC=rtpsecurity,DC=cisco,DC=com
[34]   instanceType: value = 4
[34]   whenCreated: value = 20070809124516.0Z
[34]   whenChanged: value = 20070809142528.0Z
[34]   displayName: value = matt
[34]   uSNCreated: value = 102442
[34]   uSNChanged: value = 102453
[34]   name: value = matt
[34]   objectGUID: value = .eC...aI..X....
[34]   userAccountControl: value = 66048
[34]   badPwdCount: value = 0
```

```

[34] codePage: value = 0
[34] countryCode: value = 0
[34] badPasswordTime: value = 0
[34] lastLogoff: value = 0
[34] lastLogon: value = 0
[34] pwdLastSet: value = 128311371167812500
[34] primaryGroupID: value = 513
[34] userParameters: value = m: d.
[34] objectSid: value = ..... "B.4.....K....
[34] accountExpires: value = 9223372036854775807
[34] logonCount: value = 0
[34] sAMAccountName: value = matt
[34] sAMAccountType: value = 805306368
[34] userPrincipalName: value = matt@rtpsecurity.cisco.com
[34] objectCategory: value = CN=Person,CN=Schema,
CN=Configuration,DC=rtpsecurity,DC=cisco,DC=com
[34] msNPAllowDialin: value = TRUE
[34] mapped to cVPN3000-IETF-Radius-Class: value = ALLOWACCESS
[34] Fiber exit Tx=634 bytes Rx=2217 bytes, status=1
[34] Session End

```

msNPAllowDialin is FALSE:

```

ciscoasa# debug ldap 255
debug ldap enabled at level 255
ciscoasa#
[31] Session Start

!--- Output supressed

[31] userPrincipalName: value = matt@rtpsecurity.cisco.com
[31] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,
DC=rtpsecurity,DC=cisco,DC=com
[31] msNPAllowDialin: value = FALSE
[31] mapped to cVPN3000-IETF-Radius-Class: value = NOACCESS
[31] Fiber exit Tx=634 bytes Rx=2218 bytes, status=1
[31] Session End

```

Attributes Not Mapped

The names of the attributes in this example are all case sensitive. If the LDAP attributes are not mapped to the Cisco attribute, check that the spelling in your attribute map **exactly matches** the name of the attribute sent by the LDAP server. You can see the attributes exactly as they appear from the LDAP server with the debug illustrated in the section above.

Related Information

- [Cisco Adaptive Security Appliance Support Page](#)
- [Cisco SSL VPN Client Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)