



Global Knowledge®

Expert Reference Series of White Papers

Integrating Active Directory Users with Remote VPN Clients on a Cisco ASA

Integrating Active Directory Users with Remote VPN Clients on a Cisco ASA

Chris Olsen, Global Knowledge Cisco, Microsoft, and VMware Instructor

Introduction

As our methods of doing business becomes more global and mobile, businesses large and small continue to have greater needs for traveling employees to access internal company information, securely and reliably. Cisco's widely implemented Adaptive Security Appliance (ASA) offers the functionality of secure Virtual Private Network (VPN) connectivity for remote users. While user credentials for authentication can be configured in the ASA, this creates a redundant user database for organizations that already have Microsoft Active Directory (AD) in place.

This white paper will show you how to configure an ASA to leverage AD for remote connectivity. I have done this integration several times for my clients, and they all appreciate the benefit of having only one username and password to access their internal organizational programs or data whether they are in the office or connecting remotely.

While this white paper will show you how to configure the integration between a Cisco ASA and Microsoft AD, these configuration steps will be relatively similar if you are still using the ASA predecessor, Private Internet Exchange (PIX) firewall. Microsoft has offered AD in their Windows server product versions 2000, 2003, and 2008, and this integration will work with all three versions. you will need to instal LDAP in Windows 2008 or the Internet Authentication Service (IAS) on a Windows server in your domain to accept the ASA configurations in this document.

Protocols in Use

The first underlying protocol for this integration is Lightweight Directory Access Protocol (LDAP). LDAP allows an access device, like our ASA, to **borrow** authentication from a user database such as AD. LDAP is a low-overhead protocol that runs between the ASA and AD server(s) and is not exposed to the public Internet.

The next protocol required is Authentication Authorization and Accounting (AAA). Authentication actually takes the username and password entered by the remote VPN user and verifies that it is **authentic** according to AD. Authorization establishes what the users can or cannot do inside the network once they are authorized. Accounting acts like a logging feature documenting the remote user's actions. The configuration in this paper only focuses on the Authentication portion, but does not interfere with Authorization and Accounting if those features are also desired.

Remote Access Dial in User Service (RADIUS) is used to authenticate users from the ASA to AD. RADIUS initially became popular many years ago with ISPs that had modem pools for external users to connect to their internal organizations or the public Internet with asynchronous modems. RADIUS is used in this implementation without any reference to or usage of modems.

Configuration

This example does not include all configuration commands on your ASA, just those relevant to the LDAP integration with AD. Of course, you would replace the example names and IP addresses in this document with those used in your production environment.

Once you connect into your ASA device, you will need to start your configuration in Global Config mode as follows. For this example, the hostname of your ASA device is YourASADevice.

```
YourASADevice#configure terminal
```

The following named access list called acl-vpn-nonat refers to a **virtual** internal private address space used for remote VPN users.

```
YourASADevice(config)# access-list acl-vpn-nonat extended permit ip  
any 192.168.2.0 255.255.255.0
```

The pool named remote-vpn-pool provides the range of IP addresses assigned to remote VPN users.

```
YourASADevice(config)#ip local pool remote-vpnpool 192.168.2.10-192-  
.168.2.20 mask 255.255.255.0
```

Global and NAT commands allow outside users to connect in, and inside users to connect out to the public Internet. The 192.168.1.0 address would be your internal private address space.

```
YourASADevice(config)#global (outside) 1 interface
```

```
YourASADevice(config)#nat (inside) 0 access-list acl-vpn-nonat
```

```
YourASADevice(config)#nat (inside) 1 192.168.1.0 255.255.255.0
```

RADIUS is enabled on the ASA to the LDAP AD server with the IP address 192.168.10.40 with a password of ASA123.

```
YourASADevice(config)#aaa-server RADIUS protocol radius
```

```
YourASADevice(config)#aaa-server partnerauth protocol radius  
aaa-server partnerauth (inside) host 192.168.10.40  
timeout 5  
key ASA123
```

The following Crypto commands establish the preference of security protocols for remote VPN access. When you view the running configuration on your ASA device, you will notice that some of these are the default commands:

```
YourASADevice(config)#crypto ipsec transform-set myset esp-aes esp-sha-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
```

```
YourASADevice(config)#crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
```

```
YourASADevice(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set pfs group5
```

```
YourASADevice(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
```

```
YourASADevice(config)#crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
```

```
YourASADevice(config)#crypto map outside_map interface outside
```

```
YourASADevice(config)#crypto isakmp identity address
```

```
YourASADevice(config)#crypto isakmp enable outside  
crypto isakmp policy 30  
authentication pre-share  
encryption aes  
hash sha  
group 5  
lifetime 86400
```

```
YourASADevice(config)#crypto isakmp policy 200  
authentication pre-share  
encryption aes  
hash sha  
group 2  
lifetime 86400
```

Your internal users can benefit from the DHCP services of the ASA device as shown here. DHCP on the ASA device for internal users is not required for remote VPN users.

```
YourASADevice(config)# dhcpd address 192.168.1.5-192.168.1.36 inside  
dhcpd enable inside
```

These commands demonstrate an internal WINS and DNS server or 192.168.1.90 with a domain name of YourCompany.com.

```
YourASADevice(config)# group-policy remote attributes  
wins-server value 192.168.1.90  
dns-server value 192.168.1.90  
vpn-tunnel-protocol IPSec  
password-storage disable  
ip-comp disable  
pfs enable  
default-domain value YourCompany.com
```

Tunnel groups are used to establish the settings for remote VPN users.

```
YourASADevice(config)# tunnel-group remote type remote-access
```

```
YourASADevice(config)# tunnel-group remote general-attributes  
address-pool remote-vpnpool  
authentication-server-group partnerauth  
default-group-policy remote
```

```
YourASADevice(config)# tunnel-group remote ipsec-attributes  
pre-shared-key *
```

```
YourASADevice(config)# class-map global-class  
match default-inspection-traffic
```

Conclusion

Your users will appreciate the ability to connect in to your internal network to access programs and data with the same user name and password credentials as they do when they are in the office. VPN access via the public Internet is very secure and reliable.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course(s):

[VPN – Deploying Cisco ASA VPN Solutions](#)

[SNAA – Securing Networks with ASA Advanced](#)

[ASACAMP – ASA Lab Camp](#)

For more information or to register, visit www.globalknowledge.com or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

Chris Olsen has been an IT trainer since 1993 and an independent consultant and technical writer since 1996. He has taught over 60 different IT and telephony classes to over 15,000 students. He is a technical editor for Global Knowledge's lab manuals, and he has published two books with Cisco Press, *CIPT Part 2* and *CCNA Voice Flash Cards*. He is an author and technical editor on both Microsoft OCS 2007 and 2007 R2 certification exams. He is a technical author for Cisco certified courses and is currently working on another book.