

Configuring Firewall Active Access Control

Michael J. Martin

1. What Is Active Network Access Control (ANAC)?

Most firewalls are configured to provide "passive" access control to the network. Access to the network is administered using an access policy that allows the in/out flow of traffic based on user and server network access requirements. While access needs to be explicitly defined by the network administrator, once the policy is in place, access to the permitted services is unrestricted. For most environments this approach is more than adequate. A properly configured firewall and logging infrastructure provides both the protection and auditing capabilities needed to ensure your network's security.

There are however, instances where "active" access control is needed to control access to the network. Active access control, or the more aptly descriptive interactive access control, enforces network access control on a per-user, authenticated (based on host IP address) basis. The Cisco IOS provides two mechanisms to provide this type of access control: Lock-And-Key (L&K) and Authentication Proxy (AP). Functionally, both mechanisms are similar. Both utilize AAA new-model user authentication and dynamically modify IP access group ACL's to control access. Where the two methods differ is in their operation and implementation.

2. Implementing Lock-And-Key and Authentication Proxy Access Control

L&K access control was introduced in IOS version 11.1. L&K functionality is available on most IOS implementations. But L&K is dependent on AAA new-model authentication utilizing one or a combination of local, Radius or TACACS authentication methods. When implemented, L&K blocks inbound or outbound network access. Depending on the application direction of the access group, you can use the extended access list (ACL) deny ip any any (i.e., the Lock). To access the network, a user opens a VTY session (via telnet or SSH) with the router and authenticates with a username and password (i.e., the Key). Upon successful authentication, a single dynamic permit statement is added to the interface access group. The dynamic access list entry is based on the source or destination IP address of the exec session source (again, depending on the placement of the IP access group). The dynamic entry exists for a defined period of time (based on an absolute timer or session inactivity). When the timer expires, the entry is removed. The user must then re-authenticate to access the network.

AP access control was introduced in IOS 12.0.5T. AP functionality is available as part of the IOS Firewall Feature Set (FFS) and is dependent on AAA authentication via TACACS or Radius. Local accounting is not supported. As with L&K access control, network access through the router is blocked using an inbound or outbound IP access group. While L&K requires the user to actively open a session to the router and authenticate, under AP, a user's HTTP session is passively hijacked and redirected to a java-based authentication applet. If AP access control is being imposed to protect inbound access to a secure network, the user HTTP request should be directed to an HTTP server connected to that network. If AP access control is imposed to regulate off-network access, the user just needs to open an HTTP session to any Web site and the router will intercept the request. Upon successful authentication, the router downloads user-specific access control entries and dynamically adds them to the access group's reference ACL. Hence, local user accounts cannot be utilized, because user-specific ACL customizations require the use of Radius or TACACS.

While initially it seems odd that the IOS has two methods to perform the same basic function, the method to the Cisco madness seems to be that each is rather well suited for a particular ANAC policy stance. If generic per-user access control is used to regulate access to protected resources (i.e., users utilizing public internet access to reach private resources), then L&K is a great approach. But, if the need is to control local user outbound network access (i.e., controlling user Internet access), then AP has some distinct advantages. The main one is AP's

Configuring Firewall Active Access Control

Michael J. Martin

ability to create custom per-user access control policies. Both approaches have some quirks, but both are great tools to have in your security toolkit.

3. Configuring Lock-And-Key Access Control

There are two ways to implement L&K. The first, and most common, is to utilize local authorization. The second is to utilize remote (i.e., TACACS/Radius) authorization. The local authorization approach has the advantage of using both local and remote user authentication databases. But it has the downside of having to configure use-specific VTY and corresponding AAA authentication method lists. This limits the access method for authentication to telnet. SSH cannot be used with VTY rotaries. The remote authorization approach removes the option for using local authentication databases and will work with the "default" AAA authentication and VTY configuration. The remote authorization method also makes it possible to utilize both SSH and telnet for authentication access to the router. We will examine configuring both the local and remote authorization approaches. Then, you can decide which approach is best suited for you needs.

4. L&K With Local Authorization

The local method has three configuration steps:

- Configure user authentication
- Configure VTY rotaries
- Configure the L&K access filter

All of these steps need to be done using a serial connection to the console port of the router. If you try to configure this over the network, you risk locking yourself out of the router.

5. Configuring User Authentication

In most cases, a global AAA authentication statement using the "default" named list is adequate for controlling exec shell authentication. However, since L&K uses the VTY access component of the router to facilitate access authentication along with exec shell access for administration, distinct AAA authentication policies for L&K and administration need to be created and applied to use specific VTY rotary groups. The AAA configuration for "local" is the following:

First, enable AAA and configure the authentication server:

```
aaa new-model
tacacs-server host 172.30.1.2
tacacs-server key secretkey
ip tacacs source-interface ethernet 1/0
username routeradmin password ****
! When using AAA, you should always have a local admin account.
```

Once AAA is enabled and the server has be configured, create the authentication lists:

```
aaa authentication login ANAC group tacacs+
aaa authentication login admin group local
```

In addition to authentication, it is highly recommended that login attempts be controlled, and that both access success and failures be logged to the accounting server.

```
aaa authentication attempts login 1
```

Configuring Firewall Active Access Control

Michael J. Martin

```
aaa accounting exec ANAC start-stop group tacacs+
aaa accounting send stop-record authentication failure
```

6. Configure VTY Rotaries

A rotary is a group of VTY/TTY interfaces under a common configuration policy. By default, all VTY interfaces belong to a single rotary group that listens for connections on the default protocol service ports as defined by the transport input VTY line def. For example, a VTY can be configured like this:

```
line vty 0
transport input telnet
line vty 1
transport input ssh
line vty 2 4
transport input telnet
```

The router would accept telnet and SSH connections using their default ports on this interface. In operational terms, the above VTY configuration would allow only one SSH connection (on VTY1) and four telnet VTY connections (VTY 0, 2, 3 and 4).

When using L&K, the users that need to authenticate connect via telnet (or SSH) using the known service port. To facilitate that, we need to configure the number of VTYS that we want available. The router comes with five VTYS by default; we will configure the first four to user authentication. The first we configure as the VTY transport protocol:

```
line vty 0 3
transport input telnet
```

That is followed by the authentication list configuration:

```
login authentication ANAC
```

The last step is to enable dynamic ACL editing:

```
autocommand access-enable host time 10
```

The line configuration command <autocommand {command}> sets the port to perform a specific command once the user has been authenticated. When the command has been executed completely, the session is terminated. Autocommand is commonly used when creating out-of-band terminal server configurations. SSH and telnet sessions to specific hosts are configured on the ports. When a user connects to the port, the telnet/SSH session is started. When the user ends the telnet/SSH session, the VTY session is also severed. In the case of L&K configuration, the <access-enable host timeout {1-9999 min}> command is executed, which adds dynamic ACL entries using the source address of the VTY session. Of course, for the command to work you need to have an IP access group configured to use a dynamic ACL. That brings us to the last configuration step, creating the access filter.

Hold on a second, you must still access the router to perform administration functions. We can't forget that! Since AAA is enabled and no default authentication method list has been created, all of the ports on the router that are not specifically configured are locked out,

Configuring Firewall Active Access Control

Michael J. Martin

including the console port. Before you configure the administrative VTY, configure the console port:

```
line con 0
privilege level 15
login authentication admin
```

Once the console is squared away, configure the administrative VTY in the following manner. First, define the transport protocol:

```
line vty 4
transport input telnet
transport output telnet
! This will allow you to open telnet sessions to other hosts
```

Follow that with the authentication list configuration:

```
Login authentication admin
```

The final step is to assign the VTY to a rotary group.

```
rotary 1
```

The IOS supports 99 VTY rotary groups. To connect to a rotary group using telnet, you need to specify the rotary group number starting on port 3000. So to connect to our administrative rotary, we would telnet to port 3001.

```
Outland:admin#telnet lab-router 3001
```

```
Trying 172.30.71.1...
Connected to lab-router.
Escape character is '^['.
```

```
Username:
```

Now that we can administer the router and the user authentication access has been configured, we can move on to the final step, the set-up of the access filter.

7. Configure The L&K Access Filter

The L&K access list is quite simple. You need to permit access to the router for the two rotaries and block everything else:

```
Access-list 100 permit tcp any host 172.30.1.1 eq telnet
Access-list 100 permit tcp any host 172.30.1.1 eq 3001
```

The example access list above is quite sparse. For most environments, you will want to consider permitting ICMP echo and echo-reply so that the router can ping and be pinged. Environments that utilize IPsec or Generic Route Encapsulation Protocol (GRE) tunneling will also need to permit GRE, ESP, AH, and IKE (UDP port 500). Regardless of what additional protocol support your site may need, the permit rules need to be included before the dynamic ACL statement, of which there can be only one. The IOS will ignore any additional dynamic ACL statements beyond the first. To enable dynamic additions, end the ACL with the following:

Configuring Firewall Active Access Control

Michael J. Martin

```
Access-list 100 dynamic L&K timeout 20 permit ip any any
```

There are a few points in the ACL stanza that you need to understand. The command syntax looks like this: <access-list {ACL#} dynamic {dynamic list name} timeout {1-9999 min} {permit|deny} {protocol} {source addr} {destination addr} {options}>. Most of the syntax is straightforward, but the "dynamic list name" and "timeout" need some clarification. The dynamic list name is simply a tag; it is not used for anything but it needs to be defined. The timeout value is the absolute timeout for the dynamic entry. The idle timeout is set by the access-enable command. The absolute timeout is set in the dynamic statement. If you do not set an absolute timeout, there is a possibility that the dynamic entry will not be removed. Be sure to set one. The standard eight-hour day would be 480 minutes.

Once the list has been created, install it as a standard access control filter using the <ip access-group> command:

```
interface E0/1
ip address 172.30.1.1 255.255.255.0
ip access-list 100 in
```

When the list is in place, you are ready to test. Simply telnet to the router and supply your username and password. If you authenticate successfully, the router will end the session and you should be able to access hosts on the other side. If you want to see the dynamic entries and how long they have until the expire, use the <show access-lists> command:

```
Extended IP access-list 100
Permit tcp any host 172.30.1.1 eq telnet
Permit tcp any host 172.30.1.1 eq 3001
Dynamic L&K permit ip any any
permit ip host 192.44.67.5 any (2 matches) (time left 454)
```

8. L&K with Remote Authorization

The configuration of local and remote authorization basically follows the same path, with only a few exceptions. Rather than go through the whole configuration again, we will just look at the differences between the two configurations.

9. No Administrative Rotary

For L&K to function, the user must run the <access-enable> command in the exec shell. Under the local authorization approach, this is done as a VTY <autocommand> option. The <access-enable> command is a standard exec shell command. So, in theory, (and practice) a user could just log in to the router, run the command and exit. The dynamic statement would be added and function appropriately. Of course, you would need to allow every user at least privilege level one access to the router. That's not a very secure approach, hence the use of the autocommand statement. When remote authentication is enabled, the VTYs are all configured to use the default rotary and TACACS/Radius is used to execute the <access-enable> statement.

10. TACACS/Radius Authorization

The March 2003 edition of the Router Expert covered the details on implementing TACACS authorization. For L&K remote authorization, only exec shell authorization is needed. Here is the complete IOS AAA configuration for the L&K remote model:

Configuring Firewall Active Access Control

Michael J. Martin

```
aaa authentication login ANAC group tacacs+
aaa authentication login admin group local
aaa authorization exec ANAC group tacacs+
aaa authentication attempts login 1
aaa accounting exec ANAC start-stop group tacacs+
aaa accounting send stop-record authentication failure
```

Enabling TACACS/RADIUS authorization only sets the stage. It's in the user profile configuration where the magic happens. The local authorization model depends on the VTY for command execution. With remote, TACACS/Radius passes the command to the VTY line. Here is a user profile syntax example for the tac_plus TACACS+ server:

```
user = sam{
    login = cleartext "apassword"
    service = exec {
        priv-lvl = 15
    }
    autocmd = "access-enable host timeout 10"
}
```

Aside from the need for user profile modifications on the TACACS server, the L&K configuration otherwise is the same. Users who require exec shell access for administration will need different accounts for L&K access and administration. Alternatively, these users can also run from the exec shell.

That wraps up introducing you to ANAC and Lock-and-Key access control. Next month, we will return with the final installment on configuring CBAC. As always, I hope you found this information helpful and please feel free to send questions, comments, or article ideas. Don't forget to tune in next time -- same bat time, same bat channel.