Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing the Cisco Local Director

A major risk of implementing network appliance load balancers can be the default or improperly configured network services on the device itself. Most load balancers have at least one interface in the same subnet as the Web servers for which they balance the load. If this interface, for example, is configured to run an SNMP server with a default or easily guessable read-write community string, and a hacker was to exploit the one vulnerable system mentioned above, chances are it would only be a matter of time until this ...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Securing the Cisco LocalDirector

Scott Ambrose

December 18, 2001

1.0 Introduction

In today's world of mission-critical, Web-based applications, the need for uptime and availability of these tools is one of the top requirements for organizations to both compete and succeed in this high-tech environment. Because of this fact, more and more companies are looking to design and implement highly-available, fault-tolerant infrastructures to ensure as close to 100% uptime as possible for their Web-based systems and applications. One solution organizations can implement in an effort to achieve this goal of maximum uptime is the use of network appliance load balancers. These specialized network devices typically present a single, virtual IP address and TCP or UDP port that “maps” to any number of commonly configured Web or application server IP addresses and the respective TCP or UDP service ports. This process allows for end users to connect to the virtual IP address and port while the load balancer uses one of several, configurable algorithms to determine which of the “real” servers should receive that particular connection.

This approach has two basic benefits: (1) an even distribution of load such that a high volume of traffic does not consume the computing resources of any one server, and (2) to ensure that a connection is not handed off to a server that is unavailable. However, coupled with the inherent benefits of implementing a network appliance load balancer are a number of risks which, if not addressed, can reduce, or completely eliminate, any of the perceived benefits of these appliances. For example, access to a virtual IP address and port through the perimeter defenses now also means indirect access through the perimeter defenses to each of the additional systems and services. Therefore, configuration management of the load balanced systems becomes paramount. If, for example, just one system patch is missed on one of four systems that are load balanced, a risk that could have been mitigated is now a vulnerability with roughly a 25% chance of being exploited. Just like “security by obscurity” (the absence of any true security measures in the hopes that critical systems are “ignored” or publicly “invisible”), this type of "security by percentage" is no security at all.

Another major risk of implementing network appliance load balancers can be the default or improperly configured network services on the device itself. Most load balancers have at least one interface in the same subnet as the Web servers for which they balance the load. If this interface, for example, is configured to run an SNMP server with a default or easily guessable read-write community string, and a hacker was to exploit the one vulnerable system mentioned above, chances are it would only be a matter of time until this hacker gains control of the load balancer as well. Thus, these appliances, alone, can be just as vulnerable as any other improperly configured system on a TCP/IP network.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The following paper documents specific implementation steps required to secure a well-known, widely implemented network appliance load balancer: The Cisco LocalDirector.

1.1 Assumptions of this Document

In some of the following sections I will dive in to some of the technical details and configuration tasks of making the Cisco LocalDirector more secure. Before heading down this path, I did want to mention that these security sections assume that physical security considerations and precautions have already been taken. Without ample physical security, the next two subsections can be relatively meaningless.

Additionally, a basic understanding of the OSI model, TCP/IP networks, command-line interfaces, Cisco routers, the IOS, and working knowledge of how to connect to console ports with terminal emulation software is assumed.

Finally, it should be noted that the methods and configurations outlined in this document are only intended to augment good perimeter and host-based security, not to replace them.

1.2 Brief Background of Cisco LocalDirector

The Cisco LocalDirector is a network appliance load balancer that was both the first IP load balancer on the market (1996) and the market leader in the year 2000.
(http://www.zdnet.com/products/stories/reviews/0,4161,2455836,00.html)

As stated by Cisco, “Its reliability has been proven in the highest-traffic Internet sites, and in the largest number of installations of any load-balancing device.” (http://www.cisco.com/univercd/cc/td/doc/pcat/ld.htm)

Because of the widespread popularity of the LocalDirector and the fact that none of the basic configuration steps necessary to achieve functional load balancing require modification of security parameters from their defaults, relatively insecure defaults, a custom security configuration becomes even more of a necessity.

1.3 Basic LocalDirector Network Installation

The LocalDirector acts as an Ethernet bridge between two LAN segments, requiring at least two network interfaces and operating at Layer 2 of the OSI model. These interfaces need to either be logically separated by two different VLANs in the same switch or physically separated by two different switches and two different VLANs. One interface should be placed on the same LAN segment /

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

VLAN as the gateway router. For the remainder of this document, this interface will be referred to as either the “router interface” or “interface 0”.

The second interface should be placed on the same LAN segment / VLAN as the servers and will be referred to as the “server interface” or “interface 1” for the remainder of this document.

Once the basic network installation is complete, the LocalDirector will forward or flood frames received on its “router interface” out its “server interface”.

Additionally, all configured virtual IP addresses will have the MAC address of the LocalDirector’s “router interface”. Connections initiated to a virtual server will be bridged across the LocalDirector to the real servers and connection responses from the real servers to clients will be bridge across the LocalDirector in the other direction.

1.4a Securing the Basic Installation - Upgrading the Operating System

As with any host on a TCP/IP network, the first step in securing it should be to make sure the operating system is up to date. To accomplish this task, visit http://www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/ldv42/index.htm and review the release notes for LocalDirector version 4.2. Pay specific attention to the “Open Caveats” and “Resolved Caveats” sections of the release notes. These listings will outline all critical bugs that are either in the indicated version or are resolved with the indicated version. The latest version (4.23 at the time of this writing) will almost always have the most up to date security and bug fixes implemented. For this reason, one should always use the most up to date operating system image - once the image is installed and adequately tested in a lab setting similar to the production environment, of course.

The next step is to download the operating system and Rawrite utility from the Cisco Connection Online site (NOTE: you will need to be a registered CCO user to access these files). Once these two files are downloaded to a local hard disk, the LocalDirector operating system will need to be written in a raw file system format to a floppy disk. To accomplish this task, open a DOS command prompt and change directories to the location where the downloaded files reside. At this prompt, issue the Rawrite command:

```
C:\>rawrite
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

When the following text is displayed, insert a 3.5“ floppy disk in the floppy drive and enter the name of the downloaded LocalDirector operating system:

```
RaWrite 1.2 - Write disk file to raw floppy diskette

Enter source file name: ld423.bin
```

When this process completes, remove this floppy disk, insert it in the floppy drive of the LocalDirector. Access the LocalDirector console, enter enable mode, and reload the device:

```
Welcome to LocalDirector!

Copyright (c) 1998-2000 by Cisco Systems, Inc.

        Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

        Cisco Systems, Inc.
        170 West Tasman Drive
        San Jose, California 95134-1706

localdirector> enable
Password:
localdirector# configure terminal
localdirector(config)# reload
```

When the unit reboots, it will access the floppy drive. At this time, the following console output text can be seen:

```
Booting floppy……
```

When the LocalDirector finishes booting off of the floppy, enter enable mode and issue the following command to verify that the updated operating system has been installed correctly:

```
localdirector> ena
Password:
localdirector# show version
LocalDirector 430 Version 4.2.3
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

That's all there is to it; the system is now up to date. The floppy disk can now be removed from the LocalDirector.

Now it is time to begin assessing and mitigating as many remaining risks as possible.

1.4b Securing the Basic Installation - Mitigating Access Method Risks

One of the most overlooked risks of the LocalDirector is that it does not have a separate, dedicated management interface. If it did, this interface could be placed on a secure segment of the private network, but since it does not, all remote access and administration of the LocalDirector happens via the "router interface".

The fact that the LocalDirector has it management interface on the same network segment as the servers it load balances makes other, related risks even more prevalent. First, Telnet is the only remote management utility currently available. If a hacker were to gain unauthorized access to one or more of the real servers, he or she could install a packet analyzer, more commonly referred to as a "sniffer", to watch for LocalDirector passwords traversing the network in clear-text. And while the default configuration of the LocalDirector disallows Telnet connections altogether, the LocalDirector offers no other remote management options other than direct console access.

One of the best available solutions to this design limitation is to configure a Cisco 1700, 2600, 2600, 4500, or 12000 series router as a console server by installing an NM-16A or NM-32A network module, connecting a CAB-OCTAL-ASYNC to this network module, and connecting one of the RJ45 connectors from this cable to a DB9 connector attached to the console of the LocalDirector. Once assembled and configured, this console server will allow for Reverse Telnet access to the console of the LocalDirector. Reverse Telnet is a Cisco IOS supported feature that allows Telnet connections to certain high TCP ports pass through the router and connect to tty (asynchronous) lines, such as the console port of the LocalDirector.

The Reverse Telnet solution allows the router / console server to be placed on a more secure network segment than that of the LocalDirector and real servers, but it doesn't completely mitigate the risk of passwords being sent in clear-text across the network.

To mitigate this risk, a DES or 3DES IOS image version greater than or equal to 12.2(2)T must be installed on the router / console server to replace reverse Telnet with secure shell (SSH) version 1. (NOTE: upgrading the IOS image of a router is out of the scope of this document.)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Log in to the console server, enter enable mode, turn on the password encryption service, and create a local user account:

```
router>ena
Password:
router#configure terminal
router(config)#service password-encryption
router(config)#username yourusername password yourpassword
```

Once the router / console server has the new IOS image, Each of the tty lines (there will be either 16 or 32 depending on the network module) will need to be configured in it's own rotary. The following table, excepted from http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrevssh.htm#xtocid256030, outlines both the commands necessary to finish this configuration and a brief explanation of each of the commands:

	Command	**Purpose**
Step 1	Router(config)#**line** *line-number* [*ending-line-number*]	Identifies a line for configuration and enters line configuration mode. Note: For router console configurations, each line must be defined in its own rotary, and SSH must be configured to listen in on each rotary. Note: An authentication method requiring a username and password must be configured for each line.
Step 2	Router(config-line)#**no exec**	Disables exec processing on each of the lines.
Step 3	Router(config-line)#**login** {**local** | **authentication** *listname*	Defines a login authentication mechanism for the lines. Note: The authentication method must utilize a username and password.
Step 4	Router(config-line)#**rotary** *group*	Defines a group of lines consisting or one or more lines. Note: All rotaries used must be defined, and each defined rotary must be used when SSH is enabled.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Step 5	Router(config-line)#**transport input** {**all** | **ssh**}	Defines which protocols to use to connect to a specific line of the router.
Step 6	Router(config-line)#**exit**	Exits line configuration mode.
Step 7	Router(config)#**ip ssh port** *portnum* **rotary** *group*	Enables secure network access to the tty lines. Use this command to connect the *portnum* argument with the rotary *group* argument, which is associated with a line or group of lines. Note: The *group* argument must correspond with the **rotary** *group* number chosen in Step 4.

(NOTE: some content was deleted from this table for formatting purposes)

To verify that the newly configured SSH server is working, simply use an SSH client (that supports SSH version 1) to connect to the router / console server on the port configured from Step 7 above.

It should be noted that while Secure Shell version 1 offers the advantage of encrypting sensitive network traffic such as passwords, it has also been fraught with security vulnerabilities that can be exploited with relative ease. The Cisco IOS, unfortunately, does not yet support the more secure SSH version 2.

1.4c Securing the Basic Installation - SNMP

While the LocalDirector operating system disallows telnet connections from all hosts as part of its default configuration, the SNMP defaults are not quite as restrictive. Although SNMP management stations cannot poll or send SNMP traps until the `snmp-server host` command is configured, traps are enabled by default in the LocalDirector. Additionally, the default configuration sets the default SNMP community string to 'public'. The following steps should be taken to make sure the SNMP settings of the LocalDirector are more secure.

If the LocalDirector won't be sending SNMP traps to a management station, this capability can be disabled:

```
localdirector(config)#no snmp server enable traps
```

The SNMP server itself can't be disabled on the LocalDirector, so it may be advisable to change the community string to something that would make it harder

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

for a would-be attacker to go after the LocalDirector with an SNMP brute force attack:

```
localdirector(config)#snmp-server comm string y0urString
```

1.5 Advanced Security Configurations – Protecting Your Servers

Some of the advanced security features of the LocalDirector can help add a layer of defense between the rest of the world and the servers it is load balancing, but some of these features do have drawbacks ranging in severity; these features should not be used as a replacement for good system and perimeter security.

When configuring the LocalDirector for load balancing services, the first steps are typically to create the virtual server and designate the real servers:

```
localdirector(config)#virtual 10.10.10.12
localdirector(config)#real 10.10.10.10
localdirector(config)#real 10.10.10.11
```

These example configuration commands will cause the real servers to be balanced by the virtual for all traffic.

If stricter security is required on the virtual server or if all services don't need to be load balanced, a feature called SecureBind or Port-bound Servers will block all traffic to the virtual IP address other than the protocol-specific traffic explicity configured:

```
localdirector(config)#virtual 10.10.10.12:80
localdirector(config)#real 10.10.10.10:80
localdirector(config)#real 10.10.10.11:80
```

In this particular case, any TCP connection attempts to the virtual IP address, other than those attempting connections to TCP port 80, will be met with a TCP reset.

Speaking of TCP resets, the LocalDirector can also provide limited protection against SYN Flood attacks on the virtual IP address. This functionality, called Synguard, keeps track of the number of TCP SYN requests from a client to a virtual server that has yet not responded with a SYN/ACK combination. To configure Synguard mode on a virtual server, issue the following command:

```
localdirector(config)#synguard 10.10.10.12:80:0:tcp 400
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

When the configurable threshold of SYN requests is met, the LocalDirector enters Synguard mode and begins cleaning up these half-open TCP connections is configured on a per virtual address basis:

The above command would enable Synguard on that particular virtual server, and Synguard mode would take effect when 400 half-open TCP connections are initiated to that virtual server. (NOTE: Once the LocalDirector goes into Synguard mode, it must be manually reset by changing the Synguard threshold to 0)

While SecureBind and Synguard may help secure the virtual address, they do nothing to add a layer of security to the real servers, as all traffic on the LAN can still be bridged through the LocalDirector. If an extra layer of security for the real servers is desirable, a feature called SecureBridge can be enabled. By enabling SecureBridge, traffic typically bridged through the LocalDirector will be blocked. This is an especially useful feature for real servers that have IP addresses that are routable on the Internet. Another added bonus on the Synguard feature is that it prevents real servers from initiating connections beyond the LocalDirector. If a real server is compromised, a hacker won't able to download tools to the server and will also not be able to attack other victims on the Internet from this server. To enable SecureBridge on a particular interface simply enter the command `secure` followed by the interface number:

```
localdirector(config)#secure 1
```

SecureBridge, as with other security features, can also hinder productivity. For example, if one of the real servers is a UNIX web server, it is configured as a Port-Bound (TCP 80) real server, and SecureBridge is enabled, an administrator would not be able to use the Secure Copy (scp) tool of the SSH suite to copy the updated site content files to the real servers. In this particular case, the SecureBridge feature could temporarily be turned off by issuing the following command:

```
localdirector(config)#no secure 1
```

If the updates are frequent, it may not be a viable option to continually disable and re-enable the SecureBridge feature. In this particular case, a feature called direct-ip can be utilized. The feature allows for a virtual server and a real server to have the same IP address, and be bound together in a one-to-one binding.

```
localdirector(config)#direct-ip 10.10.10.10:22:1:tcp is
```

This would allow for the site administrator to scp content files to the UNIX web server with SecureBridge enabled. Another LocalDirector security feature, called SecureAccess, can be configured to compliment the direct-ip feature by allowing only specified source IP addresses or networks to access the virtual server.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Traffic coming from a source address or network to a virtual server not explicitly configured by the `assign` command will be dropped:

```
localdirector(config)# assign 10.10.10.11:22:1:tcp
10.10.10.100 255.255.255.255
```

This command would only allow the site administrator's computer, with the IP address 10.10.10.100, to access TCP port 22 on the direct-ip server

While the SecureBridge feature is an added layer of security for the real servers, and there are workarounds for some of the productivity it could potentially hinder, SecureBridge may not be applicable in all environments. This feature, as mentioned above, blocks all bridged traffic for the specified interface. In this particular case, a web application running on an IIS 5.0 real server would not be able to initiate a connection to a Microsoft® SQL Server™ on TCP port 1433 on the other side of the LocalDirector. SecureBridge may not be applicable for environments with two-tiered web applications architected this way.

1.6 Summary

The Cisco LocalDirector is the oldest of the network appliance load balancers and is also one of the most widely deployed network devices in its class. The LocalDirector was launched by Cisco System in 1996 and with the exception of operating system updates with bug fixes and some new and enhanced functionality, it has not changed much since its initial release. Because of this, there are security risks including, but not limited to, an insecure access method and a missing management interface that need to be mitigated.

The LocalDirector may be showing its age, but because of external security methods available today and enhanced security features to add a layer of defense for the servers it load balances, it can be configured to augment an organization's security practices while helping to ensure high-availability for Web sites and applications.

1.7 References:

Cisco Systems – Cisco 400 Series – LocalDirector Product Overview
http://www.cisco.com/univercd/cc/td/doc/pcat/ld.htm

Cisco Systems - LocalDirector introduction
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/ldv42/421guide/42ch01.htm

Cisco Systems – Configuring LocalDirector
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/ldv42/421guide/42ch03.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Cisco Systems – LocalDirector 4.2 Command Reference
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/ldv42/421guide/42ch05.htm

Cisco Systems – LocalDirector 4.2 Release Notes
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/localdir/ldv42/index.htm

McClure, Scambray, Kurtz. "Hacking Exposed: Network Security Secrets & Solutions, Third Edition", McGraw-Hill, 2001. 237-239,510-512

Cisco Systems – SSH Terminal Line Access
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrevssh.htm

ZDNet – Cisco LocalDirector 430
http://www.zdnet.com/products/stories/reviews/0,4161,2455836,00.html

Network Computing - Seven Web Load Balancers Score With Round-The-Clock Access
http://www.networkcomputing.com/913/913r25.html

© SANS Institute 2001, Author retains full rights

Last Updated: September 3rd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced