The Honeynet PROJECT

Guide to the Honeywall CDROM Initial Setup

Last Updated: 06 May, 2004

The purpose of this guide is to assist you in planning and deploying your Honeywall gateway. It lists all the variables we will be required to complete during the Initial Setup phase. All corrections or suggestions should be sent to project@honeynet.org

Initial Setup
During the Initial Setup process, you will have to answer the following questions. By identifying these questions now (such as hostname, IP addresses, use of Snort and Snort-Inline) you can make your deployment a hopefully smoother and simpler process. This document is intended for you to fill out the answers before the actual deployment. The series of questions below are based on deploying a layer two bridge gateway. There will be several additional NAT questions if you enable a layer three routing gateway.

1. Initialize Drive
This wipes your drive and prepares it for the Honeywall installation. You will have to do this if you want to proceed. All data on the hardrive is lost during the initialization process.

2. Initial Setup Method
How do you want to proceed with the configuration.
- Floppy – Use `honeywall.conf` file from floppy for configuration
- Interview – Go through and answer series of questions to configure your Honeywall.

3. Firewall Mode
- Bridge (default) – Layer two bridging gateway
- Nat – Layer three routing gateway

4. Honeypot Public IP Addresses
Space delimited list of your honeypots IP's within your Honeynet. If you are doing NAT, then this is the list of the public or external IP addresses.

IP Addresses:_____
.

5. Broadcast address of honeypots

Broadcast Addresses:_____

6. Configure management interface (eth2)

- IP address of mgmt interface:_____
- Network Mask of mgmt interface:_____
- Default gateway of Honeywall:_____
- DNS server for Honeywall:_____
- Activate Interface now: Yes / No
- Activate Interface on reboot: Yes / No

7. Configure SSH daemon on gateway (listens on eth2)

- Port listening on:_____
- Allow root login (default is no): Yes / No
- Add user:_____
- Passwd for user (note: due to Dialog, password shows on screen)_____
- Passwd for root (note: due to Dialog, password shows on screen)_____
- Run SSH at Startup
- Start SSH now

8. Inbound Access to Mgmt Interface (eth2)

- Allowed inbound TCP ports:_____
- IP addresses that can access mgt interface:_____

9. Outbound access from Mgmt Interface (eth2)

- TCP ports gateway can initiate outbound:_____
- UDP ports gateway can initiate outbound:_____

10. Honeypots Outbound Control Limits

- Second/minute/hour/day/month
- TCP:_____
- UDP:_____
- ICMP:_____
- Other:_____
- Send packet through Snort-Inline: Yes / No
- Drop/Reject/Replace Ruleset

11. DNS for Honeypot

Often you want to allow the honeypots unlimited access to specific DNS servers so they can maintain resolution without filling up your outbound connection limits.

- Allow honeypots to access DNS unrestricted: Yes / No
- Which honeypot(s) can access DNS unrestricted:_____
- Which DNS servers do they have unrestricted DNS access to:_____

12. Email Alerts

The system has the ability to email information, including alerts of outbound activity and when a process has failed.

- Enable Email alerts: Yes / No
- Email address:_____
- Start email alerting on boot: Yes / No

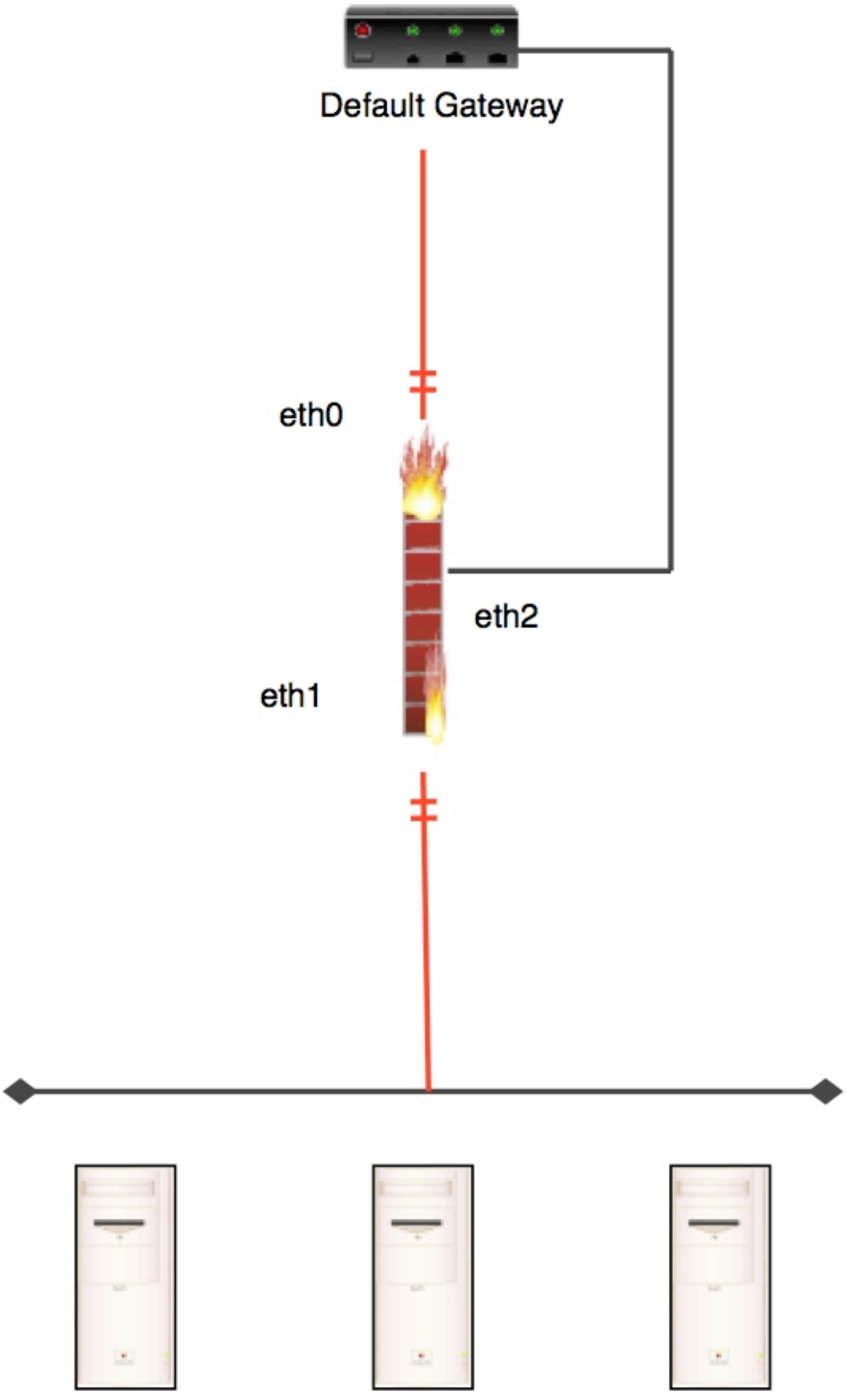
13. Sebek Packets from Honeypots

Honeypots will be sending Sebek packets over the network. We have to configure how the gateway will handle such packets. Often the default behavior is for the firewall to block the Sebek packets so the don't go past the gateway, however the Snort process listening on eth1 will collect and archive the data. You also have the option of logging each Sebek packet to /var/log/messages (can become quite chatty).

- IP destination of Sebek packets (recommend gateway of honeypots):_____
- Default UDP port of Sebek packets:_____
- Drop/Allow/Log Sebek packets

14. Hostname of gateway:_____

Reboot (your done)


Default Gateway
eth0
eth2
eth1