Installation and Deployment

GATEWAY.MANAGEMENT

Introduction

Deployment of any change in technology always requires a degree of change management appropriate to the scale of users and devices potentially impacted. This step-by-step process is not inclusive of every possible scenario and should be reviewed and customized by a system administration team which understands the full scope of deployment of this DNS-based filtering service and its included ecosystem.

Site Survey data previously gathered

This step-by-step guide assumes previous documentation was followed and all necessary data was gathered prior to activation of the software stack provided.

Maintenance window

For first-time installation, activation and customization of this software should include a 30-60 minute planned maintenance window for users and devices temporarily impacted. Advanced and experienced administrators that are able to pre-stage all lists, rules and manage a small, low-risk network, may, at their own risk, deploy without expecting any service outages.

Steps to software activation and validation

Step	Task	Comments
1	Stop DHCP on original device (if changing)	Stopping old DHCP server before a new one is started avoids DHCP broadcast conflict. It is outside of the scope of this documentation all the DHCP considerations to be made. If unsure, check with your system administration team.
2	Start DHCP on new device	DHCP on new device, if single gateway and single LAN segment, should offer both gateway and DNS at the gateway itself. For example, if the gateway is 192.168.100.1 then both gateway options as well as DNS should be offered as 192.168.100.1
3	Register an account on the cloud controller at: dashboard.gateway.management	This is an essential step in order for the on-premise software to be able to retrieve its configuration
4	Activate the software by visiting the ClearOS UI, Gateway -> Gatway.Management	This triggers the changes to dnsmasq, the interface and service creations and the firewall rules (see more details below)
5	Validate software status	From the cloud dashboard, check to make sure the router status is ONLINE (green). Failure to register should result in troubleshooting upstream communication to 72.14.247.187:443

6	Quality Assurance Checks	Choose an end-user device on which to run through these QA checks
6a	Set one device to view all logs	From the controller dashboard visit Devices -> Expand the list and locate your device -> Edit -> “Allow view all logs”
6b	Confirm “Who am I” at mytools.management/whoami	Note the device IP, MAC address and the ruleset (policy) applied
6c	Review logs at mytools.management/log	Validate entries being allowed and disallowed as expected
6d	Verify the “Dashboard” links back to your cloud dashboard	
6e	Verify the “MyBox” links back to your edge device	
7	Validate one more end-user device	Preferably a WiFi device or one that may be at an end-point of a cascaded switch to ensure that layer 2 visibility is maintained

At this point, if no further customization is applied, devices behind this configuration will all be treated with the default ruleset/policy. This is rarely sufficient, so the next set of documentation should be followed as well in order to further customize the filtering and security to the specific needs of each environment. This is especially important in an Active Directory environment where devices are now asking ClearOS to resolve AD domains. Rainbow list(s) and activations are required to restore AD and authentication functionality.

Firewall rules auto-created

As is standard with ClearOS applications, app-based firewall rules are found at this path: /etc/clearos/firewall.d

Rule	iptables	Comment
1	$IPTABLES -t filter -I [chain] 1 -p tcp -d [blockpageIP] --dport 443 -j REJECT --reject-with=tcp-reset	Along with a chain initiation rule preceding this one, this generates in a reject packet each time an https (port 443) call is made to a destination that is blocked. Rejection results in a fast end-user experience without any retry or re-resolve attempts.
2	$IPTABLES -t nat -I [chain] 1 -p tcp -d [blockpageIP] --dport 80 -j DNAT --to [blockpageIP]:6373	This one redirects block page traffic incoming on port 80 to the listener at port 6373
3	$IPTABLES -t nat -I [chain] 1 -p udp -i eth0 -o eth1 ! -d [LANIP] --dport 53 -j DNAT --to [LANIP]:53	Hijack all port 53 TCP (UDP) traffic and force it to be answered by the internal resolver. This prevents devices from circumventing DNS filtering.
4	$IPTABLES -t nat -I [chain] 1 -p tcp -i eth0 -o eth1 ! -d [LANIP] --dport 53 -j DNAT --to [LANIP]:53	Hijack all port 53 TCP (TCP) traffic and force it to be answered by the internal resolver. This prevents devices from circumventing DNS filtering.

Other Documentation

This information is provided in conjunction with other documents and videos as outlined here:

0	Product Overview and Availability
1	Procurement, Introduction and pre-installation
2	Installation and deployment (this document)
3	Lists, Rule Sets and Devices
4	Don't Talk To Strangers (DTTS)
5	Customization and Tailoring

Support

Email for support:	support@gateway.management
Technical Training available at:	http://support.gateway.management