Introduction, Pre-installation Survey and Procurement

GATEWAY.MANAGEMENT

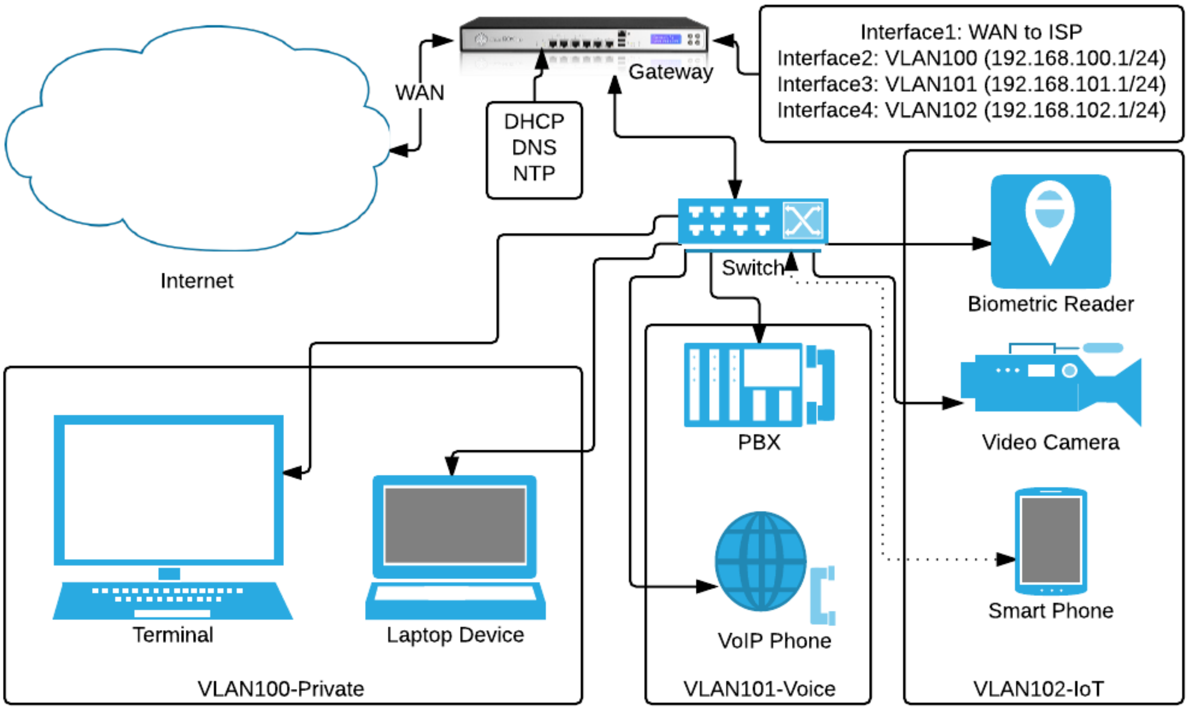
Introduction

Content filters by their very nature, interconnect with other hardware and software. The core principles on which this software is built, allows for a wide variety of deployments to occur since the fundamental product building blocks are around these key elements:

- A **DNS resolver** optimized for fast caching, deterministic answers (one device may receive a different DNS response than another, due to policy/ruleset) and multi-streaming public resolvers for fastest-possible answers
- **HTTP server** that serves core functionality including offering customizable block pages
- **iptables firewall** rules which update dynamically based on policies/rulesets
- **Cloud controller** at dashboard.gateway.management for all management
- **BrowserAssistant** available for Google Chrome from as a Chrome Browser Extension in order for blocked TLS/SSL sites to provide a better end-user experience, consider end-user Chrome Extension deployments of this extension available here:
  https://chrome.google.com/webstore/detail/block-page-assistant/pkimhjnhalcimiegkknnidjmmoiedhon

Domain	Purpose
mytools.management	LAN-facing service as a starting point for end-users looking to interact with this filter/security stack
mybox.management	LAN-facing service with valid SSL that allows for signed-certificate access to your gateway
mydns.management	WAN-facing service for dynamic DNS services

Pre-installation survey (with example)



Prior to procurement or installation, it is essential to have a clear understanding and agreement on the desired end state. It is often most easily communicated with a network diagram and annotations that illustrate the end state. A relatively simple network diagram may look like like the example offered above.

The essential details you want to include in addition to the network diagram include:

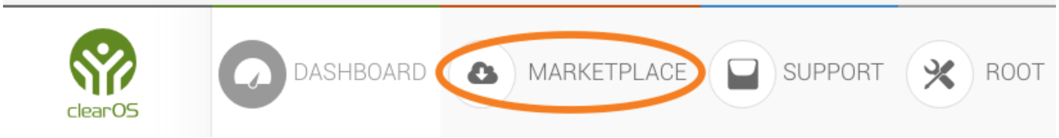
Data to collect	Why it is essential
Existing internal domains (such as mycompany.local)	Internal domains require special treatment, more information available on the Installation documentation.
Public DNS entries that resolve to the infrastructure (such as a fully qualified domain name [FQDN] which resolves to a public-facing interface and offers services, such as vpn.mycompany.com)	An often overlooked capability of DNS is to offer split-DNS for services behind a NAT gateway. Having a list of all FQDNs that resolve to a WAN-facing interface allows for an easy split-DNS provision.
Current DHCP ranges and desired changes, if any	Initial default scopes are often too small and IP resource exhaustion is an easy problem to prevent by efficiently reviewing all DHCP ranges, lease times and options.
List of all devices with statically-assigned configurations, including access credentials required	A great opportunity to optimize devices to use DHCP reservations in place of static assignments where possible.
List of PTR (reverse DNS) zones	If list is non-existent, good opportunity to establish proper PTR records for all IP ranges in use.

Current DNS servers offered internally	May need to be changed in order to reflect the use of this software stack in place of the original DNS server(s).
List of existing internal Active Directory Server(s), if any	Essential for *rainbow lists* which are essential to contain internal domains that need to be forwarded to AD for DNS resolutions (see "All about Rules, Lists, Rulesets" for further documentation).
Existing proxy server details, if any	Implications of removing proxy in favour of this filtering/security stack must be considered and planned for. For example, devices filtered via proxy may have never received a gateway before, so they will need one now. Devices previously filtered by proxy may have been provisioned manually or through group policy, which will require re-configuration.
List of all core business applications, which require WAN connectivity	In *whitelisting* mode especially, it is essential that before deployment, all required services are documented to facilitate a smooth adoption.
Verification of layer two (2) visibility, ie the gateway is able to "see" the actual MAC address of every device	This software stack "follows" device MAC addresses; an essential component to ensure policy enforcement on a per-device basis. While advanced users can advertise a non-native MAC address, the risk of this can easily be mitigated with a default policy of "No Internet" access. Default policies/rulesets are applied to newly-discovered devices.
IPv4 and IPv6 configurations	An opportunity to simplify networking.

Procurement

1. Install ClearOS 7.x or later and log onto its webconfig interface (ie https://[ClearOS-internal-IP]:81/)

2. Click on ClearOS Marketplace (as shown here):



3. Search for **Gateway.Management** and proceed with your installation.

4. Note that installation itself does not activate the service. Consult "**Installation and deployment**" for further steps.

Interfaces and Ports used

This stack has been carefully designed to avoid any interference with other uses of ClearOS. As such, full compatibility is maintained with native apache web services as well as native dnsmasq. The usage is as follows, much of it made possible by using a tun/tap adaptor:

Interface/Port	Purpose
[tuntapIP]:6373 (TCP)	Actual web server listener (is accessed via NAT firewall rule which forwards port 80 traffic to port 6373 only when hitting the tuntap interface). All other ports are rejected. In standalone mode, IP address will need to be given by user. In gateway mode, defaults to 127.27.27.27. If not available, an available IP address will be found.
127.0.0.1:5553 (UDP and TCP)	DNS resolver, which receives its traffic forwarded from dnsmasq with a configuration change of server=127.0.0.1#5553, among other changes
127.0.0.1:38473 (TCP)	To allow DNS resolver to communicate with the IP enforcement engine (DTTS)

IPv4 and IPv6

Consider the following details when implementing a dual-stacked environment. It is outside of the scope of this documentation to assess all elements within each possible configuration combination. This detail is provided to assist a network architect to make appropriate decisions around IPv4-only, IPv6-only or dual-stacked mode:

Topic	IPv4	IPv6
DNS listener	Native listener (TCP and UDP port 5553)	Native listener (TCP and UDP port 5553)
DNS hijack	End-user attempts to use any public resolver are hijacked and answered with assigned policy	End-user attempts to use any public resolver on standard port (53) are rejected (dropped)
Block page	Native listener	Implementation coming soon.

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 (this document)
2	Installation and deployment
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