Introduction and Install Checklist

Introduction

The DrawBridge is a web content filter running on the DrawBridgeOS Linux distribution (Debian-based; as-of February 2023. Units deployed prior to that timeframe were running on ClearOS, a RHEL-based distribution).

In addition to the content filter service, DrawBridgeOS can also perform the following functions:

- DHCP (enabled by default)
- DNS (enabled by default)
- Firewall (when Gateway)
- Port Forwarding (when Gateway)
- VPN server (Wireguard, OpenVPN, and IPSEC support)

DrawBridgeOS systems have one web panel

- https://draw.bridge - content filter settings

Legacy ClearOS-based DrawBridge systems have two separate web panels

- https://draw.bridge - content filter and QoS settings
- https://draw.bridge:81 - ClearOS (operating system) network configuration settings

Note: The https://draw.bridge web address is only valid inside your network (it is not reachable from other computers on the internet). If this does not work, you can also use the IP address of the unit (however you should configure your DNS properly so that it does work).

Supported client operating systems

Supported Desktop Operating Systems

- Windows
- MacOS

- Linux

Provisionally-supported Desktop Operating Systems

- ChromeOS
  (Certificate-trust is limited to the browser; key domains must be unfiltered for OS operation, therefore potentially reducing filter effectiveness.)

Supported Mobile Operating Systems

- iPhoneOS/iPadOS

Unsupported Mobile Operating Systems

- Android 7 and newer.

All operating systems **must** have the DrawBridge CA certificate installed for proper functionality!

Google products (ChromeOS and Android) limit application trust of user-installed CA certificates, therefore causing those platforms to be provisionally-supported or unsupported.

Read more: Certificate Trust Changes in Android v7 and newer

Installation Checklist

This is a high-level overview/checklist of essential tasks that need performed to install the DrawBridge on your network.

1. **Install the DrawBridge CA Certificate on all devices**: visit the Certificates panel on one of our cloud servers, below, and follow the correct steps to install the DrawBridge CA Certificate for your device.
   - Whitespire: http://whitespire.compassfoundation.io/sslcerts/dashboard/

- Sweetspire: http://sweetspire.compassfoundation.io/sslcerts/dashboard/

Whitespire

Sweetspire

2. Decide on **Installation Type**
   - Gateway (recommended)
   - Alternate Gateway
   - Proxy
3. **Collect IP addresses and credentials for existing network infrastructure equipment** (modems, routers, managed switches, wireless routers/access points, and servers) as applicable.
4. **Install the DrawBridge:** Reconfigure the network to accomodate your installation type. For example, if you opted to install as **Gateway**, replace your primary router with the DrawBridge and disable DHCP on wireless router if continuing to use it as wireless access point
5. **Ensure DNS is properly configured**:
   - Gateway setups: In most situations the DrawBridge is also the DHCP and DNS server for the network, so no additional configuration is required.
   - Alternate Gateway/Proxy setups: ensure that your local DNS server resolves the following domains to the LAN IP address of the DrawBridge:
     - `draw.bridge`
     - `<systemname>.drawbridge.systems`
     - `<systemname>.orbitmobile.network`
     - `<systemname>.passageway.id`
     - `<systemname>.compassfoundation.systems` (soon to be deprecated)
6. **Test your installation:** Navigate to popular websites to ensure they work as expected. *Getting security errors in device browsers?* Ensure the DrawBridge CA Certificate is installed as detailed in #1, above. Alternatively, you can visit your local DrawBridge web console SSL Certificates dashboard when on your DrawBridge LAN and follow the certificate installation steps.
7. **Notify your users:** Communicate to your users that their network activity is monitored and recorded. If you have company documents (eg. Employee Handbook), update as needed to properly disclose network activity monitoring and recording.

Optional:

8. **Enable remote-device access** by configuring Port Forwarding or DMZ on your modem (if not Bridged) or Firewall. Note: requires publicly-routable IP address from your Internet provider.
9. **"Harden"/Secure configuration**: (make bypassing the DrawBridge difficult)
   - Gateway setups: disable WiFi and DHCP on the (upstream) modem
   - Alternate Gateway/Proxy setups: block 80/443 TCP **and** UDP in your gateway firewall to enforce proxy settings on clients

Revision #16
Created 17 June 2022 14:13:20 by Marvin M.
Updated 1 February 2024 18:18:21 by Marvin M.