



## ADN/MACH5, EVAL & Demo Best Practices

## Preface & Deployment

- > This guide does not give a full picture of all possible scenarios, but should help with the most frequently used ones and provides useful tips for common scenarios.
- > See [Acceleration Deployment Guide](#) for more sophisticated deployment methods and detailed descriptions.
- > If possible, deploy the devices physically inline at the branch and at the core (discuss a possible WCCP solution for later).

## Software Releases

- > Use latest **SGOS 5.4.x**, or later for ProxySGs
  - Defaults in 5.3. are not set properly for many acceleration scenarios (e.g. Return-to-sender is disabled, Reflect Client IP is disabled)
  - SGOS 5.4.x offers an easy to use acceleration wizard and offers the new "Open ADN" mode
  - SGOS 5.4.x offers an extended predefined services list, which makes configuration more easy
- > Use latest **Packetwise 8.4.x**, or later for PacketShapers and load all available Plug-Ins to improve Traffic Auto-Discovery and to avoid false positives.

## SG Configuration Steps<sup>1</sup>

-> **Upgrade to 5.4 and then factory-default all boxes before you start configuration!**

**Config:** CLI command -> SG210 Series# restore-defaults factory-defaults

-> **Start with the serial console wizard to setup the device**

- **The serial console wizard** activates all needed default settings for transparent inline ADN/MACH5 deployments.

» Serial console wizard **steps 1 – 3** have to indicate:

1 = manual (aside director usage)

2 = acceleration (sets appliance defaults to WAN acceleration defaults)

3 = physically in path deployment (no WCCP)

» Serial console wizard **steps 4 – 9** implement the individual values like device name, IP-address, default gateway, DNS and admin credentials.

- **Additionally**

» Add 2nd DNS server if available/applicable

**Config:** Configuration -> Network -> Gateways & DNS Servers

» Change NTP servers if you are in a closed network and the internet cannot be reached by the ProxySG

**Config:** Configuration -> Device -> Clock -> Use Other NTP Servers

» If ProxyClient should be installed:

Switch to Managed ADN -> consult the [ProxyClient Evaluation Guide](#)

**Config:** Configuration -> Advanced Configuration -> Configuration -> ADN -> General (define a Manager...)

» Add Advertised Subnets, if Proxy Client should be tested

**Config:** Configuration -> Advanced Configuration -> Configuration -> ADN -> Routing

-> **Check License Status**

- If trial-period has expired, manually install a valid license

-> **Pre-check and double-check duplex and speed mismatches**

- Best Practice: Use 100M/full duplex, fixed (not Auto-negotiate), for all 10/100 MBit interfaces on ProxySG/router/switch ports and take care of the cabling (X-over to router, straight to switch).

**Config:** Configuration -> Network -> Adapters & Interfaces -> "Open" the appropriate IF

-> **Check interface interception and ensure "allow intercept" is only set on the LAN side**

- Maybe wrong if upgrade from 5.3 or if Proxy-edition used

**Config:** Configuration -> Network -> Adapters -> Interface Settings

### -> Check MTU Settings/Problems

- If the WAN MTU (e.g. IPSec VPNs) is lower than 1400 bytes decrease the interface MTU to avoid fragmentation
- If you do not know the WAN MTU use the ping command from a host to check which packet size can be sent over the WAN \_without\_ fragmentation.

E.g. on Windows: "ping -f -l 1472 <server-ip>" will generate a 1500 byte ICMP packet with the "Don't Fragment" Bit set. If it gets through (ping response is received) the WAN MTU is 1500 byte. If does not get through lower the value to narrow down the maximum useable MTU.

**Config:** CLI command

```
Conf t
interface 0:0
mtu-size 1350
```

- Do not enable PMTU discovery in transparent deployments (PMTU discovery on the ProxySG only works with explicit ADN tunnels)

**Config:** Configuration -> Advanced Configuration -> Configuration -> ADN -> Tunneling -> Network

### -> HTTP Cache settings

- Maximize throughput and avoid unnecessary downloads
  - » Activate the option "Enable Bandwidth Gain Mode"

**Config:** Configuration -> Advanced Configuration -> Configuration -> Proxy Settings -> HTTP Profile -> Acceleration Profile

- Avoid serving stale content
  - » Activate the option "Never Serve after Expiration"

**Config:** Configuration -> Advanced Configuration -> Configuration -> Proxy Settings -> HTTP Profile -> Acceleration Profile

### -> In Upstream-Proxy Environments

- Either use TCP-tunnel proxy to optimize traffic to the proxy
  - » Robust acceleration, but no object caching, pipelining, prefetching, etc.
- Or, if HTTP proxy is used, allow HTTP connect method to non-443 ports via VPM policy
  - » Allows full L7 HTTP proxy including object caching
  - » Do NOT use "Detect Protocol" here (breaks authentication of upstream proxy)

**Config:** Consult the knowledge base at <https://kb.bluecoat.com/> (Part of BTO) and ask for "allow http connect" to see configuration examples for explicit & transparent deployments.

-> **If deployed in a transfer network (e.g. between firewall and WAN router)**

- Check routing path to ensure that the ProxySG knows where the LAN networks are and where the WAN networks (default route), e.g. install static routes to point to the internal firewall and default route to the WAN router

**Config:** Configuration -> Advanced Configuration -> Configuration -> Network -> Routing -> Routing (select the "Install Routing Table from: Text Editor" to manually enter static routes)

-> **Use "Restrict Intercept List" to limit the optimization to known networks -> and so to minimize the risk to break "unknown" applications**

- Attention: If direct Internet access (HTTP/SMTP/POP3) should be accelerated this may not be the best solution, because public IP address then are most likely not intercepted!

**Config:** Configuration -> Advanced Configuration -> Configuration -> Services -> Proxy Services -> Restrict Intercept List (Tab)

-> **If a not-predefined service/application breaks, set the "Default"-Service to "bypass"**

**Config:** Configuration -> Advanced Configuration -> Configuration -> Services -> Proxy Services -> Group "Other"

---

<sup>1</sup> All configuration steps assume SGOS 5.4 or above and the use of the Sky UI which is the default GUI in 5.4 after the initial configuration, using the serial console wizard for WAN acceleration deployments.

## Addendum

### Documentation and Test Plan

- > At least if more than two boxes are installed, document the configuration of each box in a separate document (e.g. excel matrix) to maintain overview.
- > Get Sysinfo Files after initial deployment and as often as possible during the eval period to document configuration, logs and statistics.
- > Use the [Application Delivery Network Test Plan](#) provided from Blue Coat to document and track the performance gains, time savings and bandwidth savings in every eval.

### Recommended Reading Material / Resources

[Acceleration Deployment Guide](#)

[Web-based ADN Training](#)

[Transparent ADN with WCCP Addendum](#)

[PacketShaper Eval Guide](#)