Konfiguration des Proxy-Servers

Das Schulnetzkonzept geht davon aus, dass der Aufruf von Webseiten nur über den zwischengeschalteten Proxy möglich ist. Nur dann können mithilfe des URL-Filters squidGuard (s. weiter unten) Webseitenaufrufe via Port 80 (http) bzw. Port 443 (https) effektiv gefiltert werden. Folglich müssen alle Clients die Proxy-Informationen kennen, damit sie Webseiten laden können.

Für klassische Betriebssysteme (Windows, macOS, zahlreiche Linux-Systeme mit Desktopoberfläche) und deren Anwendungen erfragen die Proxy-Information beim DHCP-Server, sodass keinerlei Einstellungen an den Clients notwendig sind.

Die mobilen Betriebssysteme (Android, iOS, ...) unterstützen das Entdecken der Proxy-Information via DHCP leider nicht. In den W-LAN-Einstellungen des Endgeräts sind zusätzlich folgende Einstellungen zu tätigen:

- Proxy: manuell
- Proxy-Hostname: proxy.intra
- Proxy-Port: 3128

Folgende Anpassungen an den Default-Einstellungen sind zu tätigen:

Services / Web Proxy / Administration

- General Proxy Settings
  - Haken bei: Enable Proxy
  - Haken bei: Enable DNS v4 first
  - Enable access logging: Hier können Sie bei Bedarf den Zugriff auf den Proxy-Server mitloggen.
- Local Cache Settings
  - Haken bei: Enable local cache
  - Cache size in Megabytes: 10240
  - Haken bei: Enable Windows Update Cache (speichert Windows-Updates aus dem Internet zwischen und stellt sie für weitere Windows-Clients im Netzwerk bereit. Dies verringert die Belastung der Internet-Leitung durch Windows-Updates erheblich, sofern Sie keinen eigenen WSUS-Server für Windows-Updates im Einsatz haben.)
- General Forward Settings
  - Proxy Interfaces: LAN
  - Proxy Port: 3128
  - **Kein** Haken bei: Enable Transparent HTTP Proxy
    Der transparente Proxy bleibt deaktiviert, da er ohnehin nur für unverschlüsselte Webseiten (http) greifen würde.
  - **Kein** Haken bei: Enable SSL inspection
    Diese Option ist nicht zu empfehlen und in meinen Augen rechtlich mehr als fragwürdig, da sie verschlüsselte Verbindungen mit einer Man-In-The-Middle-Attacke aufbricht. Sie bleibt folglich deaktiviert.

Proxy im Netzwerk unumgänglich machen

Ausgehende Anfragen über die Ports 80 und 443 blockieren

Die beiden Haupt-Ports für Internetseitenaufrufe werden über die Firewall blockiert:

Firewall / Rules / LAN → Regeln vor den beiden "Default allow LAN ..." Regeln erzeugen:

1. Regel

- Action: Block
- Interface: LAN
- TCP/IP Version: IPv4+IPv6
- Protocol TCP/UDP
- Source: LAN net
- Destination Port Range: from: HTTP to: HTTP
- Description: z. B.: Block HTTP bypass

2. Regel

- Action: Block
- Interface: LAN
- Protocol TCP/UDP
- Source: LAN net
- Destination Port Range: from: HTTPS to: HTTPS
- Description: z. B.: Block HTTPS bypass

Von nun an können Clients nur noch dann das Internet nutzen, wenn sie den Proxy über den Port 3128 verwenden.

Proxy für bestimmte Clients umgehen

Sofern Netzwerkteilnehmer (z. B. die Serversysteme Samba, Nextcloud und Fog) nicht über den Proxy und den ggf. damit verbundenen URL-Filter das Internet nutzen sollen, müssen Sie für diese Ausnahmen in der Firewall erzeugen.

Firewall / Rules / LAN → Regeln nach der "Anti-Lockout Rule" und vor jeglichen Regeln mit der Aktion "Block" einfügen (Beispiel: uneingeschränkte Kommunikation nach außen für den Nextcloud-Server mit der IP 10.1.1.8):

- Action: Pass
- Interface: LAN
- Adress Family: IPv4
- Protocol: Any
- Source: Single host or Network: 10.1.1.8
- Destination: any
- Description: Nextcloud

Aus Gründen der Übersichtlichkeit empfiehlt es sich, unter Firewall / Aliases alle Hosts, für die eine Firewallregel gelten soll, zu einem Alias zusammenzufassen und dann für den Alias eine entsprechende Firewallregel zu erstellen.

Automatische Verteilung der Proxy-Informationen im Netzwerk

Web-Oberflächen-Zugriff auf Port 80 festlegen

Für die automatische Verteilung der Proxy-Informationen ist ein Webserver notwendig, der entsprechende Dateien über Port 80 bereitstellt. Der fachlich sauberste Weg hierfür wäre die Installation eines gesonderten Webservers. Da der Aufwand aber nicht im Verhältnis zum Nutzen steht, empfehle ich den bereits vorhandenen Webserver für die Web-Schnittstelle von OPNsense zu verwenden.

Der im OPNsense installierte Webserver lauscht standardmäßig auf Port 443. Dieser muss auf Port 80 umgestellt werden. Außerdem soll der Aufruf des Hostnamens wpad am OPNsense-Webserver als gültig definiert werden:

System / Settings / Administration / Web GUI

- Protocol: http
- Alternate Hostnames: wpad

Ein Nachteil daran ist, dass die Web-Schnittstelle nun unverschlüsselt zu erreichen ist. Durch Einsatz des Reverse-Proxy (s. später) kann man dieses Problem beheben und wieder gesichert auf die OPNsense-Einstellungen zugreifen.

PAC-Datei konfigurieren

Klassische Betriebssysteme (Windows, macOS, zahlreiche Linux-Systeme mit Desktopoberfläche) entnehmen die Proxy-Information einer Datei namens wpad.dat. OPNsense bietet eine Möglichkeit, diese Datei über die Web-Schnittstelle zu konfigurieren.

Folgendes Beispiel zeigt eine PAC-Konfiguration, welche Clients für sämtliche externe Anfragen den Proxy benutzen lässt. Lediglich interne IP-Adressen und URLs werden direkt angefragt.

Services / Web Proxy / Administration / Proxy Auto-Config / Matches

1. Match (Vollständige Hostnamen)

- Name: is_fqdn
- Negate: Haken (Verneinung des Match Types)
- Match Type: Plain Hostname (No dots inside)

2. Match (Nicht interne Anfragen)

- Name: not_internal
- Negate: Haken (Verneinung des Match Types)
- Match Type: Hostname Matches
- Host Pattern: z. B. *.schulnetz.intra

3. Match (Nicht IP aus dem Bereich 10/8)

- Name: not_ipin_10/8
- Negate: Haken (Verneinung des Match Types)
- Match Type: IP Is In Network
- Network: 10.0.0.0/8

3. Match (Nicht IP aus dem Bereich 172.16/12)

- Name: not_ipin_172.16/12
- Negate: Haken (Verneinung des Match Types)
- Match Type: IP Is In Network
- Network: 172.16.0.0/12

4. Match (Nicht IP aus dem Bereich 192.168/16)

- Name: not_ipin_192.168/16
- Negate: Haken (Verneinung des Match Types)
- Match Type: IP Is In Network
- Network: 192.168.0.0/16

5. Match (Nicht IP aus dem Bereich 127.0.0/24)

- Name: not_ipin_127.0.0/24
- Negate: Haken (Verneinung des Match Types)
- Match Type: IP Is In Network
- Network: 127.0.0.0/24

Services / Web Proxy / Administration / Proxy Auto-Config / Proxies

1. Proxy (LAN-Proxy des OPNsense)

- Name: lan-proxy
- Proxy Type: Proxy
- URL: <opnsense-lan-ip>:3128

Services / Web Proxy / Administration / Proxy Auto-Config / Rules

- Haken bei Enabled
- Name: not-internal-to-proxy
- Matches: is_fqdn, not_internal, not_ipin_10/8, not_ipin_172.16/12, not_ipin_192.168/16, not_ipin_127.0.0/24
- Join Type: And
- Math Type: If
- Proxies: lan-proxy

Nachdem alle Objekte angelegt wurden, wird die PAC-Datei durch anklicken des orangen Neu-Laden-Symbols neu erstellt und steht z. B. unter http://<opnsense-ip>/wpad.dat zur Verfügung.

DHCP-Server-Einstellungen

Damit Clients bei Verbindung ins Schulnetz nun vom DHCP-Server den Ort der PAC-Datei erfahren, müssen an diesem entsprechende Einstellungen vorgenommen werden:

Services / DHCPv4 / [LAN] / WPAD → Haken bei: Enable Web Proxy Auto Discovery

DNS-Weiterleitungen

Einige Programme nutzen nicht die vom System via DHCP eingefangenen Proxy-Informationen. Vielmehr suchen sie selbst unter folgenden URLs - bei der Annahme, dass schulnetz.intra die Schuldomain ist - nach der Datei wpad.dat:

- http://wpad.schulnetz.intra/wpad.dat
- http://wpad/wpad.dat

Damit die Namensauflösung für diese URL funktioniert müssen im DNS-Server des OPNsense entsprechende Einträge hinterlegt werden:

Services / Unbound DNS / Overrides

- Host: schulnetz / Domain: intra / Type: A or AAAA / IP: 10.1.1.1 (OPNsense-IP)
- Host: wpad / Domain: schulnetz.intra / Type: A or AAAA / IP: 10.1.1.1 (OPNsense-IP)
- Host: <leer> / Domain: wpad / Type: A or AAAA / IP: 10.1.1.1 (OPNsense-IP)

Eine zusätzliche Weiterleitung empfiehlt sich für die Einstellung des Proxys auf mobilen Endgeräten. Hier sollte aus diversen Gründen bei der Einstellung Proxy-Host nicht die IP-Adresse von OPNsense sondern ein Hostname wie z. B. proxy.intra angegeben werden:

- Host: proxy / Domain: intra / Type: A or AAAA / IP: 10.1.1.1 (OPNsense-IP)