Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративный Squid-прокси: контроль интернета для офиса

Разбираем наш стенд: squid-openssl, Kerberos SSO, ACL по отделам, выборочный SSL Bump и отчёты SARG

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Офисный канал забит стримингом и скачиваниями, CRM и 1С тормозят, а при инциденте (фишинг, шифровальщик) невозможно установить, кто и когда ходил на вредоносный домен — логов интернет-активности нет. Мы решаем это корпоративным Squid: explicit-прокси с AD-аутентификацией, категорийной фильтрацией, лимитами скорости и полугодовым архивом логов — без затрат на лицензии NGFW.

Почему это важно бизнесу

- Один автоплей видео съедает 6–8 ГБ за день; десяток таких — и канал 100 Мбит/с встал, менеджеры ждут CRM
- Без прокси-логов расследование заражения невозможно: неизвестно, кто скачал вредонос и что могло утечь
- Squid закрывает до 80 % задач NGFW при нуле затрат на лицензии — экономия сотен тысяч рублей за 5 лет
- Мониторинг без подписанных уведомлений (ст. 86 ТК РФ, 152-ФЗ) — судебный риск при увольнениях

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.6

актуальный стабильный релиз Squid (08.06.2026) — ориентир, если собираем из исходников

squid-cache.org, 2026

6.13

пакет squid-openssl в Debian 13 — ставим его: базовый squid собран без поддержки SSL Bump

packages.debian.org

20

children 20 startup=5 idle=5 для auth-хелперов: дефолтных 5 не хватает на утренний пик логинов

наш стандарт

2 hours

credentialsttl Basic-LDAP: кэш проверки пароля — баланс нагрузки на DC и скорости отзыва доступа

по докам Squid

16MB

dynamic_cert_mem_cache_size (дефолт 4MB): кэш сгенерированных сертификатов при SSL Bump

по докам Squid + наш стандарт

32

дефолт sslcrtd_children по докам; на 130 рабочих мест нам хватает 8 startup=2 idle=2

по докам Squid

РЕАЛИЗАЦИЯ 1 ИЗ 3

Базовый контур: squid-openssl, ACL по отделам, delay pools

Что настраиваем

Отдельная VM Debian: 4 vCPU, 8 ГБ RAM, 100 ГБ SSD — офис 30–150 рабочих мест

Как мы это делаем

1. apt install squid-openssl sarg apache2; инициализация кэша squid -z; кэш держим 5–10 ГБ — HTTPS не кэшируется, старые «50 ГБ» бессмысленны
2. ACL: src-сети отделов (10.10.x.0/24), категории dstdomain из /etc/squid/acl/*.txt (social, video, torrent, malware), время time MTWHF 09:00-18:00
3. Порядок http_access: deny malware/adult → allow белый список (ФНС, банки, 1С) → политики отделов → deny all последним
4. delay_pools class 2 (aggregate/individual в байт/с): 6 250 000/125 000 на архивы, отдельный пул на видеохостинги

РЕЗУЛЬТАТ

Канал в пиковые часы разгружается со 100 % до 60–65 %, тяжёлые скачивания не душат CRM и 1С; политика доступа читается как таблица и меняется правкой txt-списков без перезапуска — squid -k reconfigure

КЛЮЧЕВОЙ НЮАНС

http_access срабатывает по первому совпадению: блокировки — выше разрешений, deny all — всегда последним, иначе одна строка открывает всё

РЕАЛИЗАЦИЯ 2 ИЗ 3

SSO по Kerberos и права по AD-группам

Что настраиваем

Интеграция с Active Directory: keytab, negotiate-хелпер, external ACL, раздача через GPO и WPAD

Как мы это делаем

1. msktutil --create --service HTTP/proxy.<fqdn> --enctypes 0x18 → keytab; владелец proxy, права 600
2. auth_param negotiate program negotiate_kerberos_auth -k keytab -s HTTP/<fqdn>; children 20 startup=5 idle=5, keep_alive on
3. external_acl_type ad_group %LOGIN ext_kerberos_ldap_group_acl; acl grp_finance external ad_group «Proxy-Finance-Restricted» и т.п. по отделам
4. Раздача: GPO Registry (ProxyEnable, ProxyServer :3128) + WPAD — A-запись wpad и DHCP option 252 на wpad.dat

РЕЗУЛЬТАТ

Сотрудник один раз логинится в Windows — пароль прокси больше нигде не вводится; перевод человека между отделами = перенос между AD-группами, squid.conf не трогаем

КЛЮЧЕВОЙ НЮАНС

SPN HTTP/<fqdn> обязан совпадать с именем, по которому браузер зовёт прокси: адрес по IP ломает Negotiate и роняет клиентов в Basic

РЕАЛИЗАЦИЯ 3 ИЗ 3

Выборочный SSL Bump и отчётность SARG

Что настраиваем

HTTPS-инспекция на том же узле: свой CA, динамическая генерация сертификатов, HTML-отчёты

Как мы это делаем

1. Свой CA rsa:4096 на 3650 дней; база сертификатов security_file_certgen -c -s ssl_db -M 64MB; CA в Trusted Root через GPO
2. http_port 3128 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=16MB; sslcrtd_children 8 startup=2 idle=2
3. Логика: ssl_bump peek step1 all → splice по списку исключений (банки, госуслуги, мессенджеры) → bump all
4. SARG по cron: дневной отчёт 23:55, недельный по пн, месячный 1-го числа; отчёты за Apache с Basic-auth и TLS

РЕЗУЛЬТАТ

Видны полные URL внутри HTTPS, отчёт для ИБ-аудитора собирается за минуты вместо недель; обращения к фишинговым доменам блокируются и фиксируются поимённо

КЛЮЧЕВОЙ НЮАНС

peek серверного сертификата на step2 исключает bump на step3 — peek держим только на step1; до включения подписываем уведомления о мониторинге (ст. 86 ТК РФ)

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Пакет squid вместо squid-openssl**
  В Debian дефолтный squid собран с GnuTLS и не поддерживает ssl-bump; для HTTPS-инспекции ставим только squid-openssl (проверка: squid -v → --with-openssl)

- ✕ **Дефолтные children у auth-хелперов**
  basic children 5 (дефолт) забивается очередью на утреннем пике — 407-е ответы и «висящие» страницы; ставим 20 startup=5 idle=5

- ✕ **peek на шаге 2 SSL Bump**
  По докам peek серверного сертификата на step2 почти всегда исключает bump на step3 — остаётся только splice; peek применяем на step1

- ✕ **Аутентификация на transparent-прокси**
  На портах intercept/tproxy auth отключена самим Squid — клиент не знает о прокси; логин пользователей работает только в explicit-схеме

- ✕ **Гигантский дисковый кэш**
  HTTPS-трафик не кэшируется, огромный cache_dir лишь замедляет запуск и ребилд индекса; 5–10 ГБ под статику достаточно

- ✕ **WPAD только через DHCP**
  Часть браузеров игнорирует option 252 и ищет wpad по DNS; публикуем оба канала — A-запись wpad + опция 252, иначе машины идут мимо прокси

- ✕ **Bump банков и госсервисов**
  Приложения с certificate pinning ломаются молча; ведём nobump-список (банки, госуслуги, мессенджеры) и ставим splice до bump all

- ✕ **Логирование без юридической базы**
  Без подписанных уведомлений (ст. 86 ТК РФ, 152-ФЗ) мониторинг оспорим в суде; шаблоны подписываем до включения логов

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- squid-openssl на отдельной VM, ACL-категории в txt-файлах, deny all последним
- Explicit-прокси :3128, настройки браузеров через GPO, доступ по src-сетям отделов
- logrotate для access.log, хранение логов 6 месяцев

НОРМАЛЬНО

- Kerberos SSO: keytab через msktutil + negotiate_kerberos_auth
- Права по AD-группам через ext_kerberos_ldap_group_acl
- WPAD (DNS + DHCP option 252), delay_pools class 2 на архивы и видео
- SARG-отчёты по cron за Apache с Basic-auth и TLS

ХОРОШО

- Выборочный SSL Bump: peek step1 → splice исключений → bump, CA через GPO
- Мониторинг прокси: squidclient mgr:info в Zabbix (hit ratio, дескрипторы)
- Резервный Squid вторым адресом в WPAD/PAC — отказоустойчивость
- Автообновление категорийных блэклистов malware и фишинга по расписанию

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Прокси вынесен на отдельную VM, а не совмещён с контроллером домена?
- [ ] Стоит squid-openssl, а не GnuTLS-сборка (squid -v показывает --with-openssl)?
- [ ] Последнее правило http_access — deny all?
- [ ] SSO работает без ввода пароля: SPN совпадает с FQDN прокси в настройках браузеров?
- [ ] Банки, госуслуги и мессенджеры в splice-списке и не перехватываются?
- [ ] access.log ротируется и хранится не менее 6 месяцев?
- [ ] Сотрудники подписали уведомление о мониторинге (ст. 86 ТК РФ, 152-ФЗ)?
- [ ] SARG-отчёты закрыты аутентификацией и TLS, доступ только у ИТ и руководства?
- [ ] Есть процедура срочного отключения SSL Bump для проблемного приложения?
- [ ] delay_pools ограничивают тяжёлые скачивания в рабочие часы?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Развернём Squid под ключ за 3 рабочих дня: VM, ACL по отделам, отчёты SARG — от 45 000 ₽ для офиса до 50 ПК
- Настроим Kerberos SSO и права по AD-группам, раскатаем настройки на все PM через GPO и WPAD
- Внедрим выборочный SSL Bump с юридическими шаблонами уведомлений для сотрудников
- Возьмём прокси на абонентку: обновление списков, отчёты, реагирование на инциденты — от 7 500 ₽/мес

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Configuration Reference: ssl_bump, sslcrtd_program, sslcrtd_children (squid-cache.org — v6–v7)

02 Configuration Reference: auth_param (children, credentialsttl, realm) (squid-cache.org — v6–v7)

03 Configuration Reference: delay_pools / delay_parameters, http_port ssl-bump (squid-cache.org — v6–v7)

04 Пакеты squid и squid-openssl в Debian 13 (trixie) (packages.debian.org — 6.13)

05 Squid Versions: стабильные релизы ветки 7.x (squid-cache.org — 2026)

06 Features/SslPeekAndSplice (wiki) (wiki.squid-cache.org — v4+)

07 Наш шаблон squid.conf для офиса 30–150 PM (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.