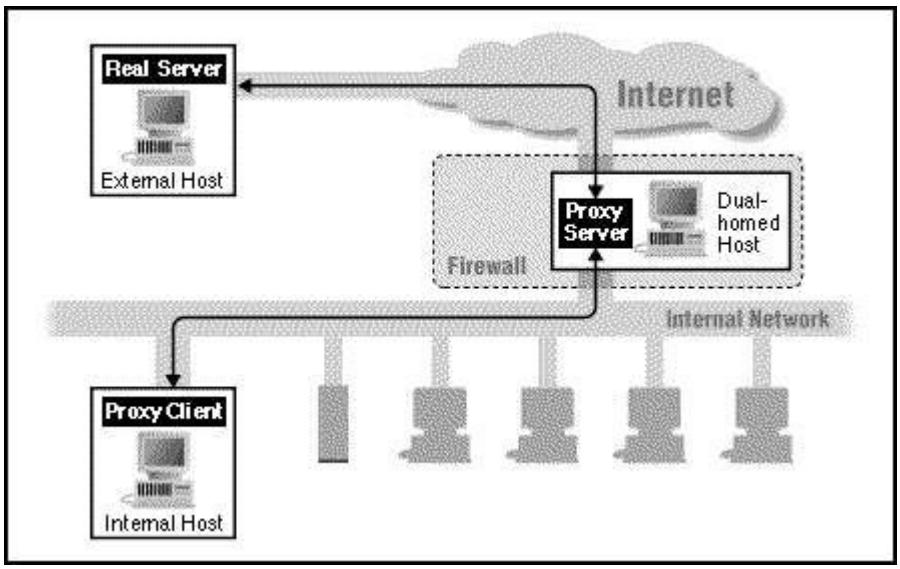
پراکسی سرور

در یک تشکیلات که از اینترنت استفاده می‌کند، یک پراکسی سرور ترکیبی از سخت‌افزار و نرم‌افزار است که بعنوان یک واسطه بین کاربر داخلی و اینترنت عمل می‌کند به طوریکه امنیت، نظارت مدیریتی و سرویس‌های caching تامین می‌شود. یک سرور پراکسی دارای پروتکل مشخصی است، بنابراین برای هرنوع پروتکلی (HTTP، FTP، Gogher و غیره) باید تنظیم شود. پراکسی سرور بعنوان بخشی از یک سرور gateway (نقطه‌ای در یک شبکه که ورودی به شبکه‌ای دیگر است) رفتار می‌کند و می‌تواند برای انجام یک یا چند فانکشن که در بخش بعد به آن اشاره می‌شود، تنظیم شود.



عملکردهایی که پراکسی سرور می‌تواند داشته باشد

با تعریفی که از یک پراکسی ارائه شد، می‌توان از پراکسی برای بهبود عملکرد یک شبکه استفاده‌هایی کرد که در اینجا به چند مورد آن به اختصار اشاره می‌کنیم:

- **Firewall (دیواره آتش)**

برای سازمانی که فایروال دارد، پراکسی سرور تقاضاهای کاربران را به فایروال می‌دهد که با آنها اجازه ورود یا خروج به شبکه داخلی را می‌دهد.

- **Caching (ذخیره سازی)**

سرور پراکسی که عمل caching را انجام می‌دهد، منابعی مانند صفحات وب و فایل‌ها را ذخیره می‌کند. هنگامی که یک منبع مورد دسترسی قرار گرفت، در سرور دخیره می‌شود و تقاضاهای بعدی برای همین منبع مشخص با محتویات cache پاسخ داده می‌شود. این عمل، دسترسی به آن منبع را برای کاربرانی که از طریق پراکسی به اینترنت متصل هستند، سرعت می‌بخشد و از طرفی از ترافیک اینترنت می‌کاهد و اجازه استفاده بهتر از پهنای باند به کاربران داده می‌شود.

- **Filtering (فیلتر کردن)**

سرور پراکسی می‌تواند ترافیک وارد شونده و خارج شونده از شبکه را بررسی کند و به آنچه که با معیارهای امنیتی یا سیاست سازمان مغایرت دارد، اجازه عبور ندهد.

- **Authentication (تصدیق هویت)**

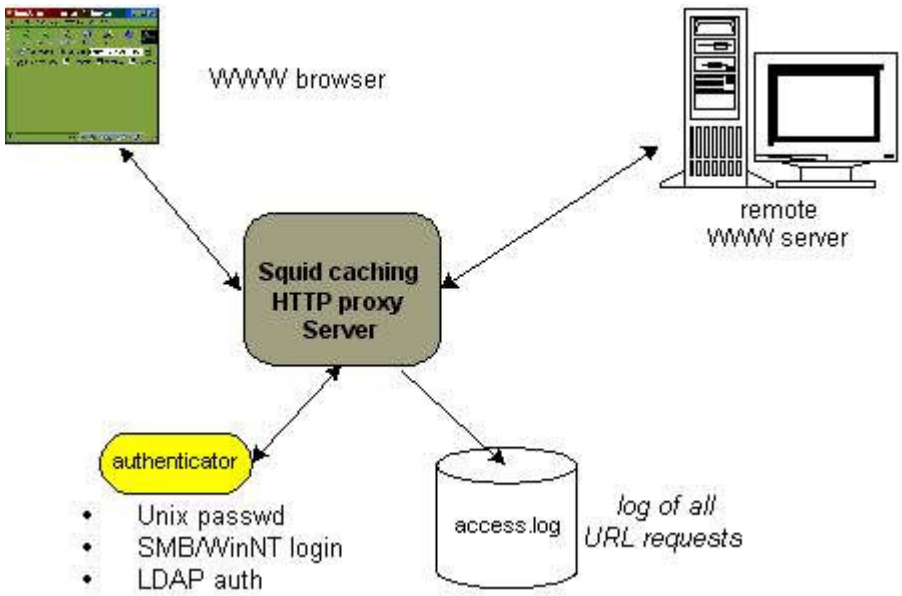
بسیاری منابع الکترونیکی سازمانی توسط ورود با کلمه رمز یا قرار داشتن در دامنه مشخصی از IP محدود شده‌اند. کاربران دور معمولاً از یک سرویس‌دهنده اینترنت ثالث استفاده می‌کنند که در این صورت این کاربر یا IP کامپیوتر آن برای سازمان معتبر تشخیص داده نمی‌شود. برای کاربرانی که بصورت فیزیکی به شبکه داخلی سازمان متصل نشده‌اند، پراکسی طوری عمل می‌کند که به کاربران دور اجازه ورود موقت داده شود یا به آنها بطور موقت یک IP سازمان تخصیص داده شود که بتوانند به منابع محدود شده دسترسی پیدا کنند.

- **Anonymization (تغییر هویت)**

برای محافظت شبکه داخلی یک سازمان از کاربران موجود در اینترنت، سرور پراکسی می‌تواند هویت سیستم‌های متقاضی داخلی را تغییر دهد. اگر منبع (مثلاً صفحه وب یا فایل) تقاضا شده توسط کاربر داخلی سازمان، در cache موجود نباشد، سرور پراکسی برای آن کاربر، بعنوان کلاینت عمل می‌کند و از یکی از آدرس‌های IP خودش برای تقاضای آن منبع از سرور موجود در اینترنت استفاده می‌کند. این آدرس IP «موقت»، آدرسی نیست که واقعاً در شبکه داخلی سازمان استفاده گردد و در نتیجه از بعضی از حمله‌های نفوذگران جلوگیری می‌شود. هنگامی که صفحه تقاضا شده، از طرف سرور روی اینترنت به پراکسی سرور می‌رسد، پراکسی سرور آن را به تقاضای اولیه مرتبط می‌کند و برای کاربر می‌فرستد. این پروسه تغییر دادن IP باعث می‌شود که تقاضا دهنده اولیه قابل ردیابی نباشد و همچنین معماری شبکه سازمان از دید بیرونی مخفی بماند.

- **Logging (ثبت کردن)**

پراکسی سرور می‌تواند تقاضاها را بهمراه اطلاعات لازم در جایی ثبت کند تا بعداً امکان پیگیری اعمال کاربران داخل سازمان فراهم شود.



پیکربندی مرورگر

- **تعامل کاربر:** کاربر باید از ابتدا مرورگر خود را پیکربندی کند که بدین ترتیب نیاز است که اطلاعات را از پشتیبانی فنی سازمان بدست آورد.
- **پیکربندی دستی:** در این پیکربندی کاربر باید سروری را که نرم‌افزار پراکسی را اجرا می‌کند، مشخص کند. کاربر باید استثنائات هر دامنه‌ای را که می‌تواند بطور مستقیم به آن وصل شود، مشخص کند و به این ترتیب در اتصال به این دامنه‌های مشخص‌شده، پراکسی در مسیر قرار نمی‌گیرد.
- **پیکربندی خودکار:** یک فایل تنظیم پیکربندی توسط سازمان که منطق استفاده از پراکسی توسط مرورگر در آن قرار دارد. URL فایل باید در پیکربندی مرورگر وارد گردد. اینکه یک تقاضا از طریق پراکسی مسیریابی شود یا خیر، بستگی به شروط موجود در آن فایل دارد.

Www.Network.Clik.IR