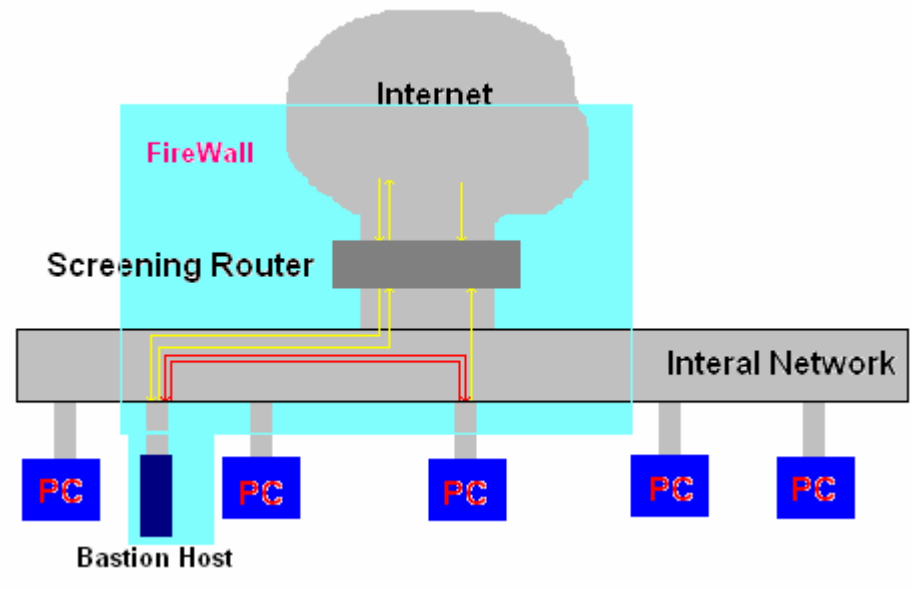
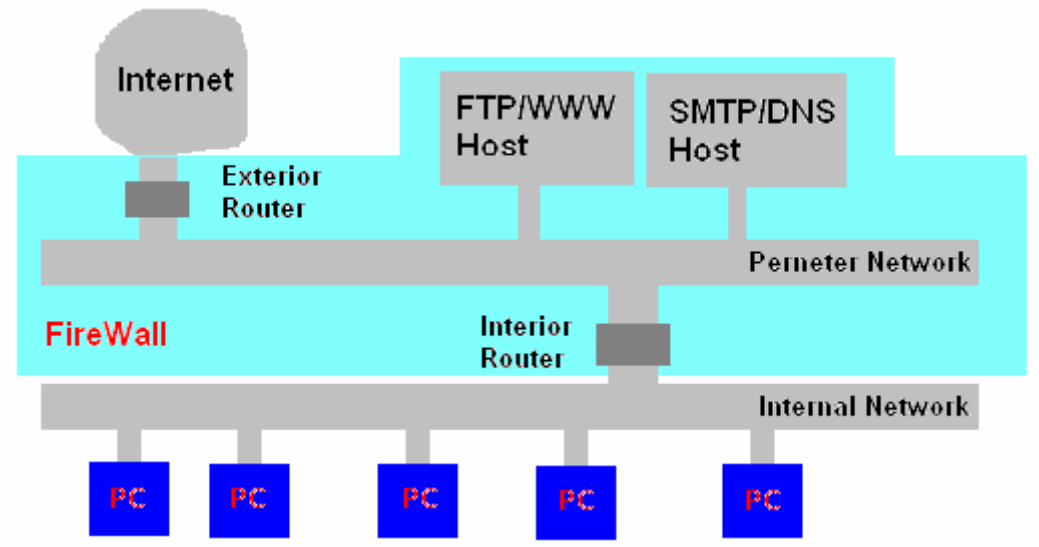
انواع فایروال از لحاظ پیکربندی

در این مقاله به صورت بصری ، چندین نوع پیکربندی توضیح داده می شود . قطعا پیکربندی های متنوع دیگری نیز برای این کار وجود دارد .
نکته : در تمامی تصاویر ، فضایی که زیر نظر فایروال هست ، به رنگ آبی مشخص شده است .

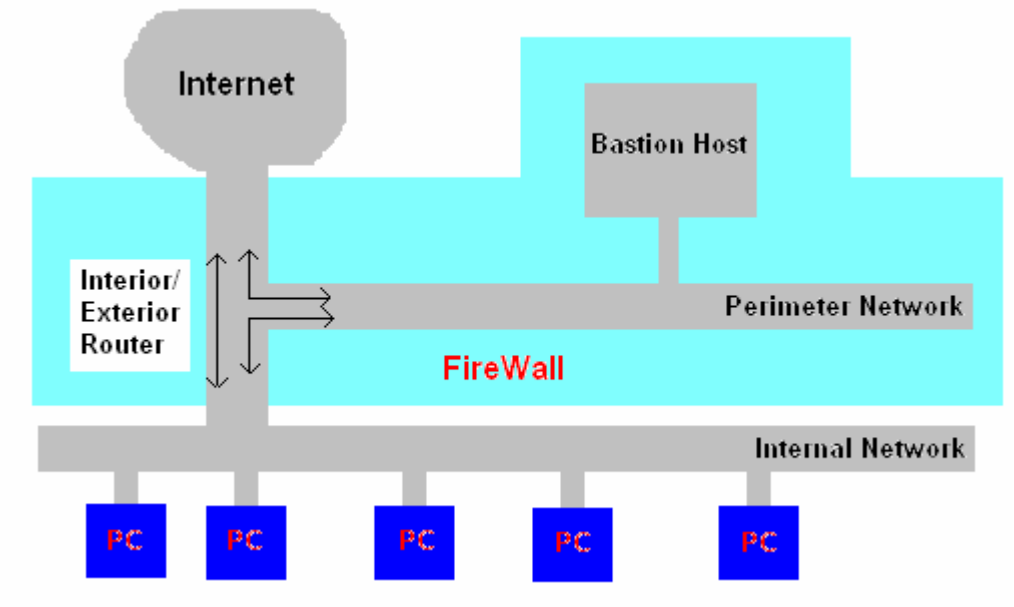


این نوع پیکربندی از ساده ترین نوع پیکربندی است که فقط شامل یک مسیریاب و یک میزبان سنگر (Bastion Host) در خود شبکه داخلی است که به همین علت از نظر درجه امنیتی ، پایین است و هکران می توانند میزبان سنگر (Bastion Host) را از شبکه جدا کنند و به راحتی به شبکه نفوذ کنند .

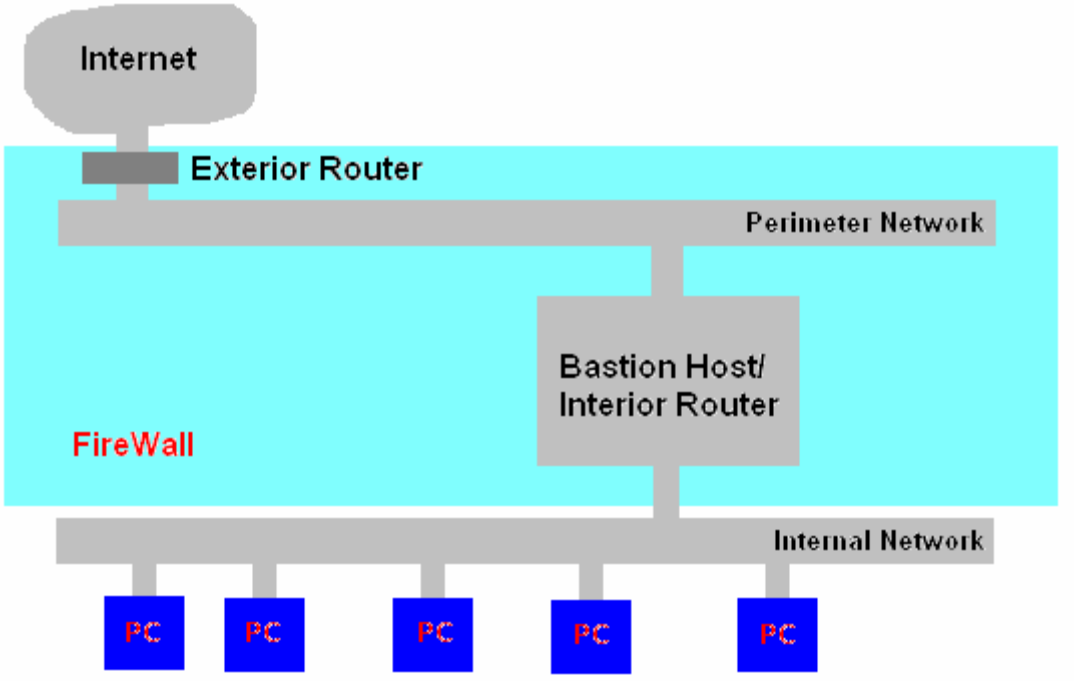


در این نوع پیکربندی ، بجای میزبان سنگر (Bastion Host) ، دو خدمات دهنده اي که بر اساس پروتکل های FTP (برای دانلود و آپلود کردن) و SMTP (برای فرستادن اطلاعات مثل Mail که بیشترشان متن است) کار می کنند ، قرار داده شده است . در این پیکربندی ، مسیریاب ها و میزبان سنگر (Bastion Host) هر یک در شبکه جداگانه اي قرار دارند .

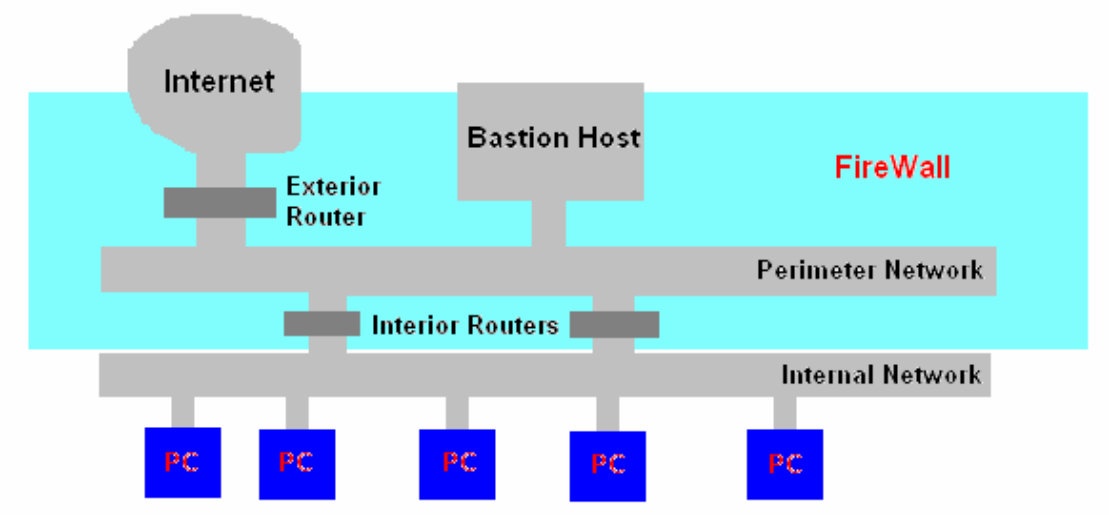
PDF-XCHANGE
Click to buy NOW!
www.docu-track.com



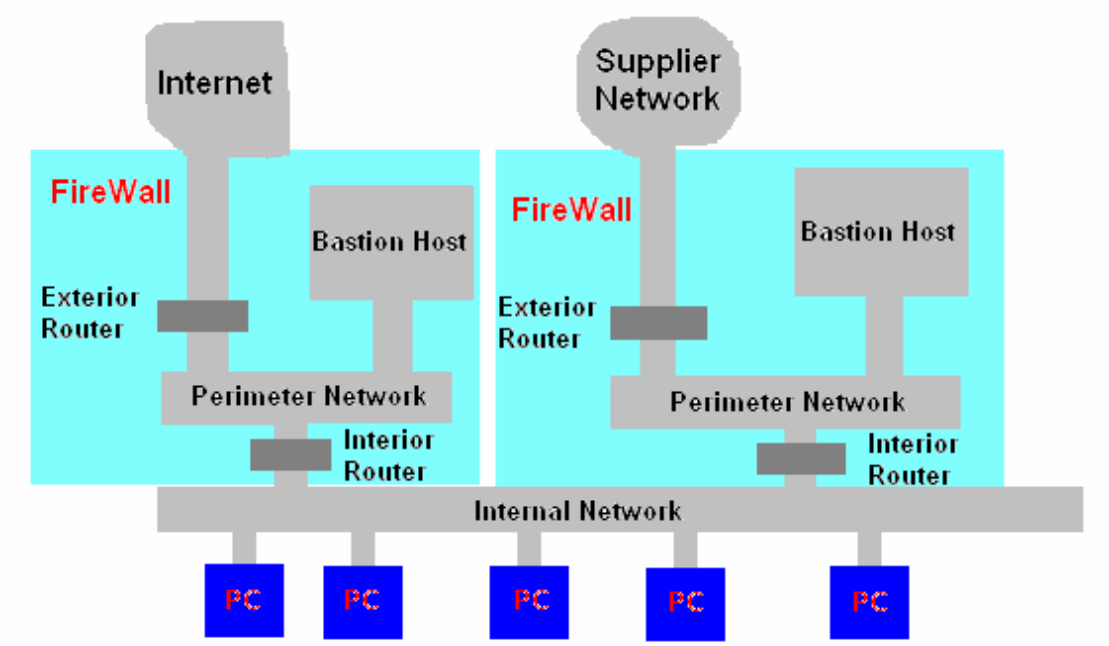
در این نوع پیکربندی ، بجای دو مسیریاب ورودی و خروجی ، فقط از یک مسیریاب استفاده می شود و همین امر باعث می شود درجه امنیت آن نسبت به پیکربندی هایی با دو مسیریاب ، کاهش یابد . ولی بعلت اینکه میزبان سنگر (Bastion Host) و مسیریاب ، در شبکه جداگانه هستند ، نسبت به پیکربندی هایی که فاقد شبکه خاص خود هستند ، امنیت بیشتری دارد .



در این پیکربندی ، فقط از یک مسیریاب استفاده شده و مسیریاب داخلی آن حذف شده . این پیکربندی نسبت به پیکربندی هایی که مسیریاب خارجی آن حذف شده ، امنیت پایینتری دارد . زیرا مسیریاب داخلی از نظر امنیتی ، پر اهمیت تر است .



در این پیکربندی برای افزایش سرعت شبکه داخلی از دو مسیریاب داخلی استفاده می شود .



در این پیکربندی ، از دو فایروال ، یکی برای حفاظت از اینترنت و دیگری برای حفاظت از شبکه خارجی استفاده می شود و دارای امنیت قابل قبولی است .

انواع فایروال از لحاظ عملکرد

۱) فایروال های سطح مدار (Circuit-Level) :

این فایروال ها به عنوان یک رله برای ارتباطات TCP عمل می کنند . آنها ارتباط TCP را با کامپیوتر پشت خود قطع می کنند و خود به جای آن کامپیوتر به پاسخگویی اولیه می پردازند . در واقع تنها پس از برقراری ارتباط است که اجازه می دهند تا داده به سمت کامپیوتر مقصد جریان پیدا کند و تنها به بسته های داده اي مرتبط اجازه عبور می دهند . این نوع از فایروالها ، هیچ داده اي درون بسته های اطلاعات را مورد بررسی قرار نمی دهند و لذا سرعت خوبی دارند . ضمناً امکان ایجاد محدودیت بر روی سایر پروتکلها (غیر از TCP) را نیز نمی دهند .

۲) فایروالهای پروکسی سرور (Proxy Server) :

فایروال های پروکسی سرور ، به بررسی بسته های اطلاعات در لایه کاربردی می پردازند . این پروکسی سرور درخواست ارایه شده توسط برنامه های کاربردی پشت خود را قطع می کند و خود به جای آنها درخواست را ارسال می کند . همچنین نتیجه درخواست را نیز از ابتدا خود دریافت و سپس برای برنامه های کاربردی ارسال می کند . این روش با جلوگیری از ارتباط مستقیم برنامه با سرورها و برنامه های کاربردی خارجی ، امنیت بالایی را تامین می کند . از آنجایی که این فایروال ها پروتکلهای سطح کاربرد را می شناسند ، لذا می توانند بر مبنای این پروتکلها ، محدودیتهایی را ایجاد کنند . همچنین آنها می توانند با بررسی محتوای بسته های داده اي ، به ایجاد محدودیتهای لازم بپردازند . البته این سطح بررسی می تواند به کندی این فایروال ها بیانجامد . همچنین از آنجایی که این فایروالها باید ترافیک ورودی و اطلاعات برنامه های کاربردی کاربر انتهایی را پردازش کنند ، کارایی آنها بیشتر کاهش می یابد . اغلب اوقات پروکسی سرورها از دید کاربر انتهایی شفاف نیستند و کاربر مجبور است تغییراتی را در برنامه خود ایجاد کند تا بتواند به طور دایم فایروال ها را به کار گیرد . در عین حال هر برنامه جدیدی که بخواهد از این نوع فایروال عبور کند ، باید تغییراتی را در پشته پروتکل فایروال ایجاد کرد .

۳) فیلترهای Nosstateful Packet :

این فیلترها روش کار ساده اي دارند . آنها بر مسیر یک شبکه می نشینند و با استفاده از مجموعه اي از قواعد ، به بعضی بسته ها اجازه عبور می دهند و بعضی دیگر را بلوکه می کنند . این تصمیم ها با توجه به اطلاعات آدرس دهی موجود در پروتکلهای لایه شبکه ، مانند IP و در بعضی موارد با توجه به اطلاعات موجود در پروتکلهای لایه انتقال ، مانند سرآیندهای TCP و UDP اتخاذ می شود . این فیلترها زمانی می توانند به خوبی عمل کنند که فهم خوبی از کاربرد سرویس های مورد نیاز شبکه جهت محافظت داشته باشند . همچنین این فیلترها می توانند سریع باشند ، چون همانند پروکسی ها عمل نمی کنند و اطلاعاتی درباره پروتکلهای لایه کاربرد ندارند .

۴) فیلترهای Stateful Packet :

این فیلترها بسیار باهوشتر از فیلترهای ساده هستند . آنها تقریباً تمامی ترافیک ورودی را بلوکه می کنند ، اما می توانند به ماشینهای پشت خود اجازه بدهند تا به پاسخگویی بپردازند . آنها این کار را با نگهداری رکورد اتصالاتی که ماشینهای پشتشان در لایه انتقال ایجاد می کنند ، انجام می دهند . این فیلترها ، مکانیزم اصلی مورد استفاده جهت پیاده سازی فایروال در شبکه های مدرن هستند . این فیلترها می توانند رد پای اطلاعات مختلف را از طریق بسته هایی که در حال عبورند ، ثبت کنند . ناگفته نماند ، بسیاری از فیلترهای جدید Stateful می توانند پروتکلهای لایه کاربرد مانند FTP و HTTP را تشخیص دهند و لذا می توانند اعمال کنترول دسترسی را با توجه به نیاز ها و سرعت این پروتکلها انجام دهند .

۵) فایروالهای شخصی :

فایروالهای شخصی ، فایروالهایی هستند که بر روی کامپیوترهای شخصی نصب می شوند . آنها برای مقابله با حملات شبکه اي طراحی شده اند . این گونه فایروال ها ، معمولاً از برنامه های در حال اجرا در ماشین آگاهی دارند و تنها به ارتباطات ایجاد شده توسط این برنامه ها اجازه می دهند که به کار بپردازند . نصب یک فایروال شخصی بر روی یک PC بسیار مفید است ، زیرا سطح امنیت پیشنهادی توسط فایروال شبکه را افزایش می دهد . از طرف دیگر از آنجایی که امروزه بسیاری از حملات در واقع از درون خود شبکه حفاظت شده انجام می شوند ، بنابراین فایروال شبکه نمی تواند کاری برای آنها انجام دهد و لذا یک فایروال شخصی بسیار مفیدتر خواهد بود . همچنین معمولاً نیازی به تغییر برنامه جهت عبور از فایروال شخصی نصب شده (همانند پروکسی) نیست .

با تشکر ، شهروز