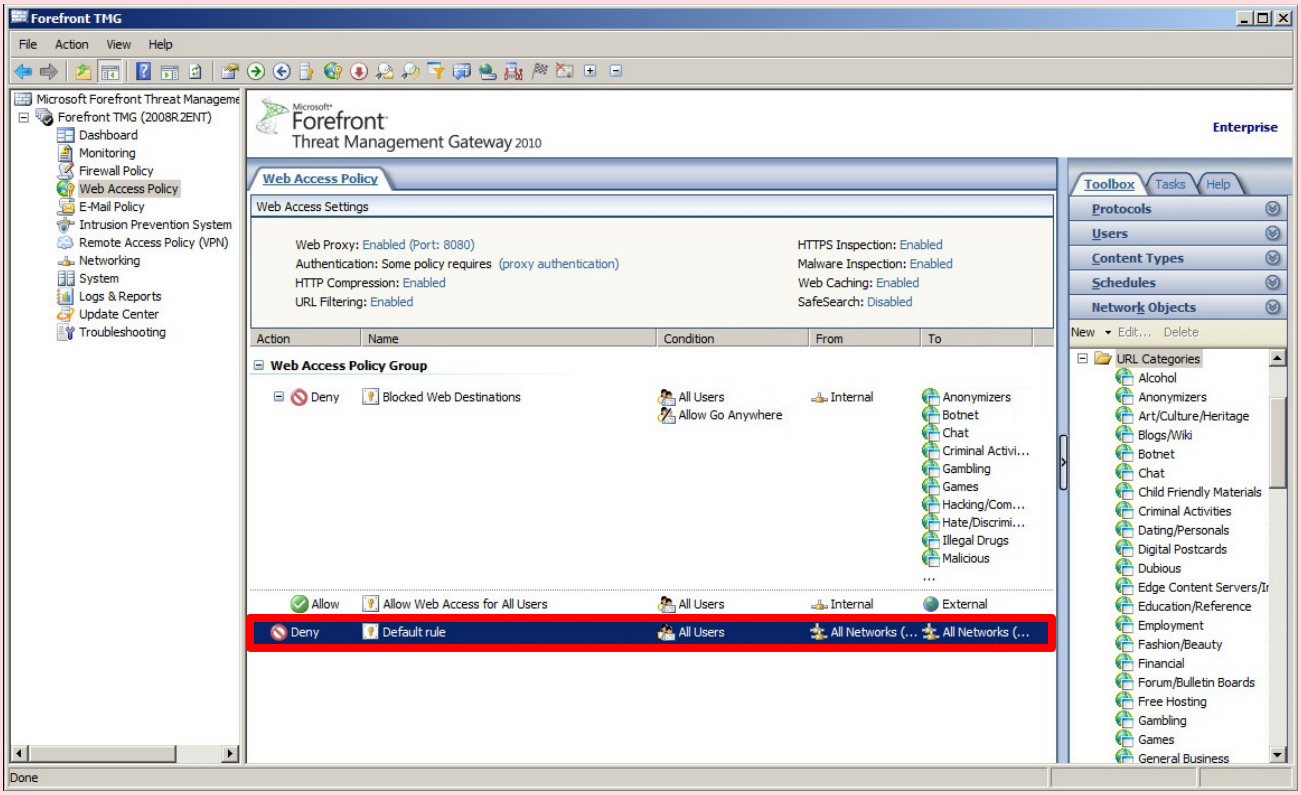
نمونه ایی از کتاب الکترونیکی آموزش

Forefront TMG 2010

Web Access Policy نود

به کنسول TMG و نود Web Access Policy باز می گردیم:



همانطور که مشاهده می کنید همراه با رول Deny، که دسترسی به لیستی از URL ها را بلاک نموده است، به صورت اتوماتیک یک رول با دسترسی Allow برای All Users، نیز بر روی ترافیکهای HTTP و HTTPS ایجاد شده است که از طریق این رول دسترسی کاربران به همه سایتهای HTTP و HTTPS به جز

لیست URL های بلاک شده، برقرار می شود. برای مشخص کردن چگونگی دریافت اینترنت توسط کلاینتها، می بایست با انواع کلاینتهای TMG و روشهای مختلف دریافت اینترنت آشنا شوید که در ادامه به توضیح این موارد خواهیم پرداخت.

توجه:

به صورت پیش فرض بعد از نصب نسخه های فایروال قدیمی ISA، تمامی ترافیکها به سمت تمامی شبکه ها مسدود می شد و به منظور باز کردن ترافیک ISA و شبکه داخلی به اینترنت، می بایست یک Access Rule از شبکه های Internal و Local Host به شبکه External تعریف می کردید، اما در TMG 2010 بعد از ایجاد رول Web Access Policy یک رول Allow نیز به صورت اتوماتیک ایجاد می شود.

علاوه بر آن در TMG نیز همانند ISA، هیچ یک از کامپیوترها نمی توانند TMG را Ping کنند مگر اینکه امکان استفاده از دستور Ping به کلاینتها داده شود که به دلایل امنیتی و توضیحات بیشتری که در تنظیمات نود Intrusion Prevention System داده خواهد شد، اجازه استفاده از دستور Ping توسط کاربران صحیح نمی باشد.

توجه

اگر رول Web Access policy را تعریف نمی کردید، یک رول پیش فرض با دسترسی Deny از All Networks (and Local Host) به All Networks (and Local Host) با انتخاب نودهای Firewall Policy و Web Access policy قابل مشاهده بود که تمامی ترافیکها را از تمامی شبکه ها و Local Host (به TMG شبکهLocal Host خطاب می شود) به یکدیگر و به شبکه های خارجی و اینترنت بلاک کرده است. این رول را در شکل قبل مشخص کرده ایم.

بعد از ایجاد رول Web Access Policy، اگر نود Firewall Policy را انتخاب کنید، رول ایجاد شده در گروهی با عنوان Web Access Policy Group قرار گرفته است که ترتیب اعمال رولهای این گروه به ترتیب شماره هایی که در کنار آنها مشخص شده است، می باشد.

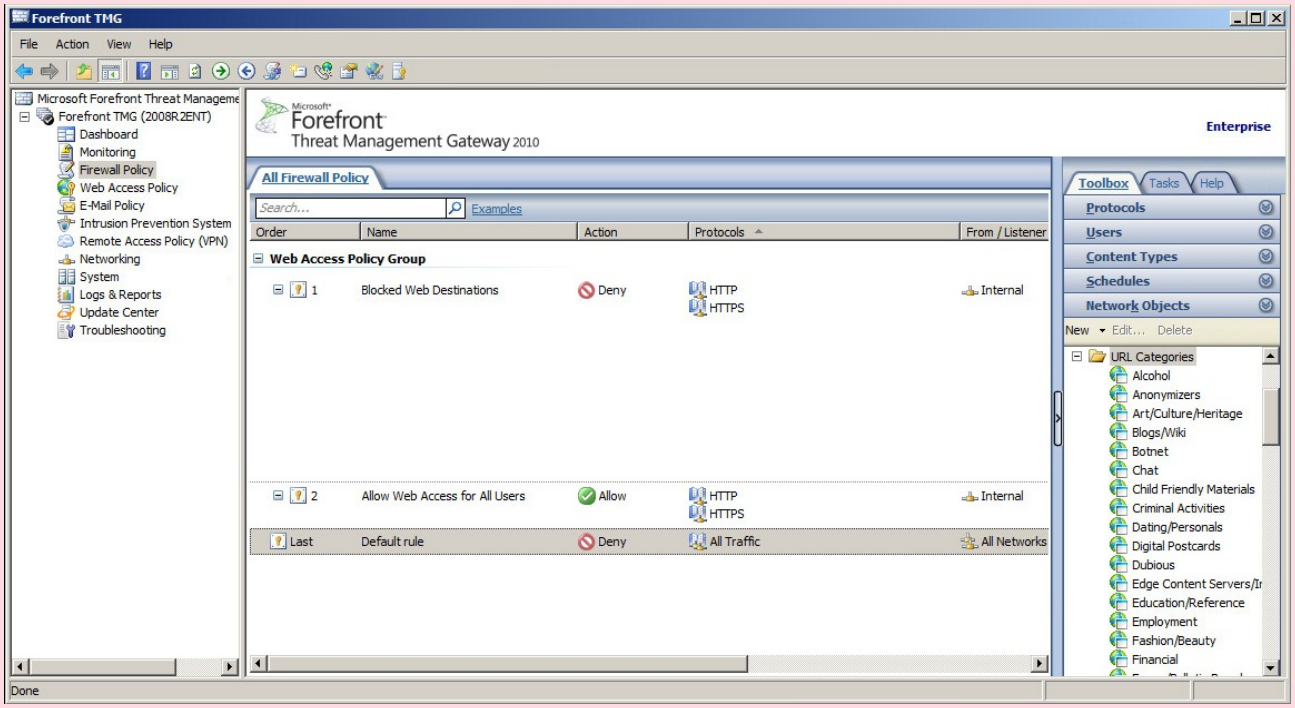
همانطور که مشاهده می کنید ابتدا رول Deny قرار گرفته است که دسترسی محدودتری را بر روی دسته ای از URL های درخواستی با ترافیکهای HTTP و HTTPS دارا می باشد و سپس رول Allow با دسترسی ALL به همه ترافیکهای HTTP و HTTPS قراردارد،که بعد از رول Deny قرار گرفته است.

به طور کلی ترتیب قرارگیری Access Rule ها در ترتیب اعمال آنها مهم بوده و ابتدا ترافیکهای با دسترسی محدودتر کنترل و اعمال می شوند.

دلیل منطقی این عملکرد نیز به این صورت است که Access Rule های ایجاد شده به ترتیب از بالا به پایین بررسی می شوند و اگر شما رول با دسترسی Allow را در ابتدا قرار دهید به دلیل Allow بودن ترافیک های مورد نظر در آن رول، به این ترافیک ها اجازه عبور داده می شود و رول با دسترسی Deny برای عبور همان ترافیک، اعمال نخواهد شد. بنابراین می بایست در ترتیب قرار دادن رولها دقت کنید.

برای مثالی در این زمینه، تصور کنید در شرکت یا سازمان خود کاربری داریم که عضو دو گروه متفاوت می باشد که یکی از این گروه ها با دسترسی Allow و دیگری با دسترسی Deny است.

پس اگر بخواهید اجازه دسترسی به کاربر مورد نظر داده شود می بایست رول Allow را که کاربر مورد نظر در آن قرار گرفته است در ابتدا قرار دهید و بالعکس، در صورتی که بخواهید اجازه دسترسی های این کاربر بلاک شود، رول Deny را که این کاربر در آن قرار گرفته است در ابتدا قرار دهید .



رول Firewall Client، را در فصل های بعد به صورت مفصل بررسی خواهیم کرد.

این مبحث قسمتی از مطالب مختص به کتاب الکترونیکی آموزش TMG 2010 که توسط گروه آموزشی فرزان تولید شده است، می باشد.

WWW.Modir-Shabake.com