SOPHOS

Cybersecurity made simple.

راهنمای مقاوم‌سازی محصولات Sophos XG Firewall

بر اساس توصیه‌نامه مرکز مـاهـر

شبکه گستر

امنیت شما | وظیفه ما

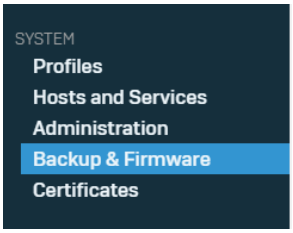
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) توصیه‌نامه‌ای برای امن‌سازی سامانه‌های فناوری اطلاعات در مقابل تهدیدات سایبری احتمالی همزمان با ۱۳ آبان ماه منتشر کرده که در آن طی ۱۰ بند مواردی جهت مقاوم‌سازی سامانه‌ها ارائه شده است.

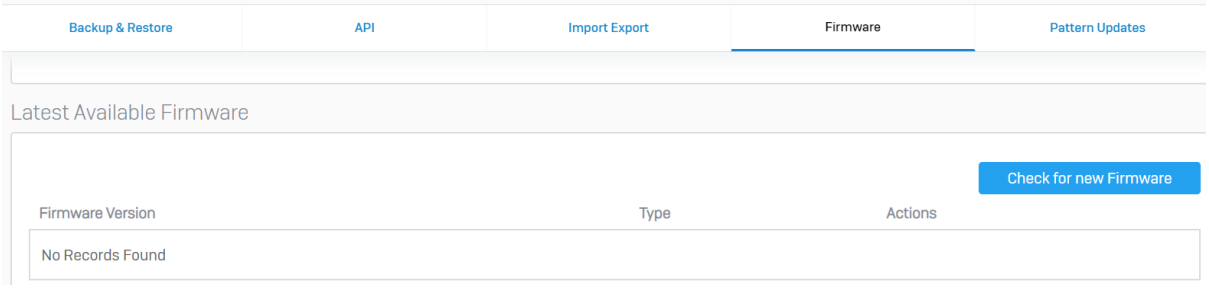
شرکت مهندسی شبکه گستر هم‌راستا با توصیه‌نامه فوق اقدام به انتشار راهنمای مقاوم‌سازی محصولات خود مطابق با بندهای مورد اشاره مرکز ماهر کرده است.

در این راهنما نحوه بررسی تنظیمات Sophos XG Firewall در جهت اجرای توصیه‌های مرکز ماهر ارائه گردیده است.

به‌روزرسانی سیستم عامل و نرم‌افزارها

فایروال سوفوس تنها برند فایروال معتبر جهانی است که به‌روزرسانی آن برای نشانی‌های IP ایران هیچ محدودیتی ندارد و بطور مستقیم و برخط انجام می‌شود. برای اطمینان از به‌روز بودن ثابت‌افزار[1] و داده‌های امنیتی فایروال می‌توان در منوی System > Backup & Firmware در کنسول تحت وب دستگاه به صفحات Firmware و Pattern Updates مراجعه کرد.

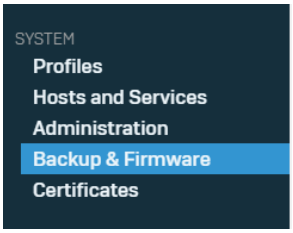


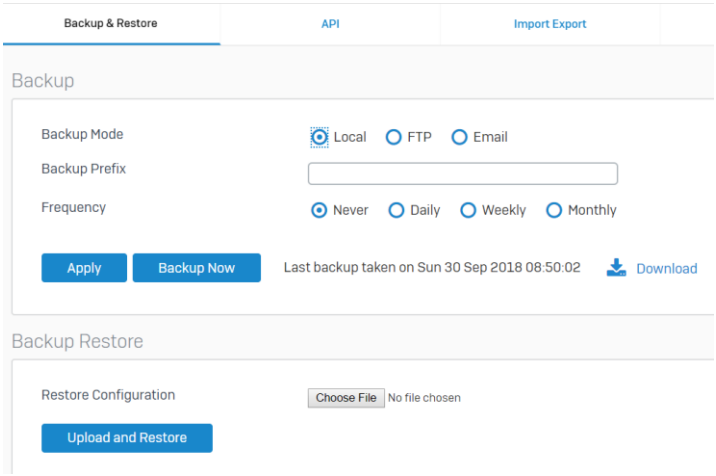


تهیه و نگهداری نسخه پشتیبان

برای تهیه نسخه پشتیبان از تنظیمات فایروال سوفوس، می‌بایست از منوی System > Backup & Firmware به صفحه Backup & Restore مراجعه کرد.

[1] Firmware



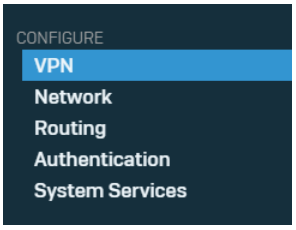


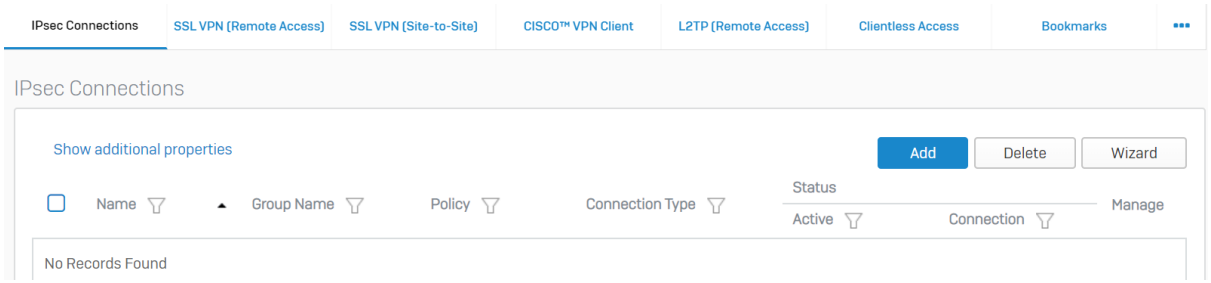
بهره‌گیری از رمزنگاری مناسب در تبادل اطلاعات

فایروال سوفوس پودمان‌های متنوعی از VPN را ارائه می‌دهد که می‌توان از آنها برای رمزنگاری در تبادل اطلاعات استفاده کرد. جدول زیر فهرست پودمان‌های قابل استفاده در این تجهیزات را نشان می‌دهد.

Site to Site VPN Protocols	Remote Access VPN Protocols
IPSec	IPSec
SSL	PPTP
RED (Sophos proprietary)	L2TP
	SSL
	HTML5

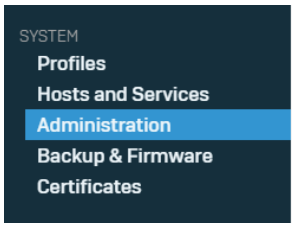
برای راه‌اندازی ارتباطات VPN می‌توان به منوی Configure > VPN مراجعه کرد.

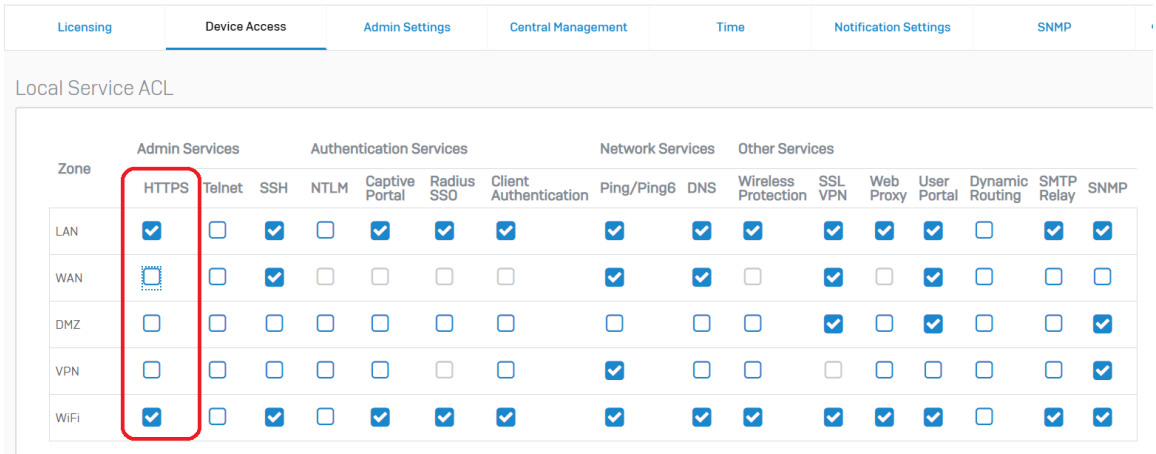




اتخاذ راه‌حل برای دسترسی ایمن از راه دور برای مدیریت سرویس‌ها و زیرساخت‌ها

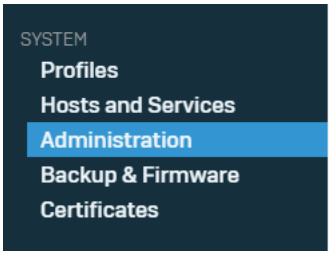
برای دسترسی از راه دور به کنسول فایروال سوفوس می‌توان تنظیمات لازم را در صفحه Device Access از منوی System > Administration اعمال کرد. با Set/Reset کردن گزینه HTTPS برای محدوده‌های مختلف، دسترسی به کنسول تحت وب دستگاه از Zone مورد نظر باز یا بسته خواهد شد.

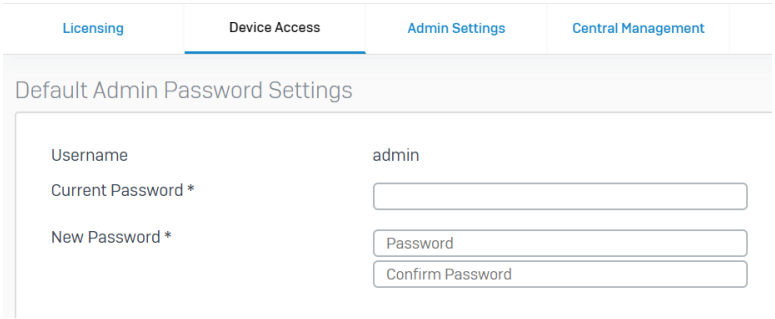




اتخاذ مکانیزم احراز هویت و رمز عبور قوی

رمز ورود به فایروال را در صفحه Device Access از منوی System > Administration می‌توان تغییر داد. توصیه می‌شود رمزهای عبور، پیچیده[۲] و حاوی بیش از ۱۰ نویسه[۳] باشند تا امکان نفوذ و دسترسی غیرمجاز به فایروال که Gateway اصلی شبکه تلقی می‌شود به حداقل برسد.

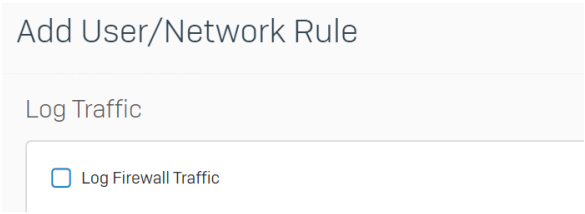




جمع‌آوری، نگهداری و بررسی رخدادنماها

جمع‌آوری و نگهداری لاگ در زمان بروز حوادث امنیتی، کمک شایانی به ردگیری و پیدا کردن نفوذگران و متخلفان می‌کند. بنابراین توصیه می‌شود که تا حد ممکن دسترسی به منابع مهم و اصلی شبکه ثبت و لاگ شوند. البته باید ظرفیت حافظه داخلی فایروال برای ثبت و نگهداری لاگ نیز مد نظر قرار گیرد. در صورت نیاز به نگهداری حجم زیاد لاگ برای مدت طولانی توصیه می‌شود از محصول جانبی سوفوس بنام iView که مخصوص نگهداری لاگ و گزارش‌ها طراحی شده، استفاده شود.

برای فعال کردن لاگ دسترسی به منابع شبکه، باید در قواعد فایروال گزینه Log Firewall Traffic فعال شود.

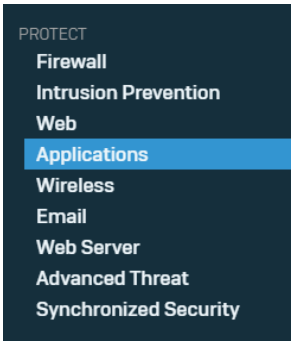


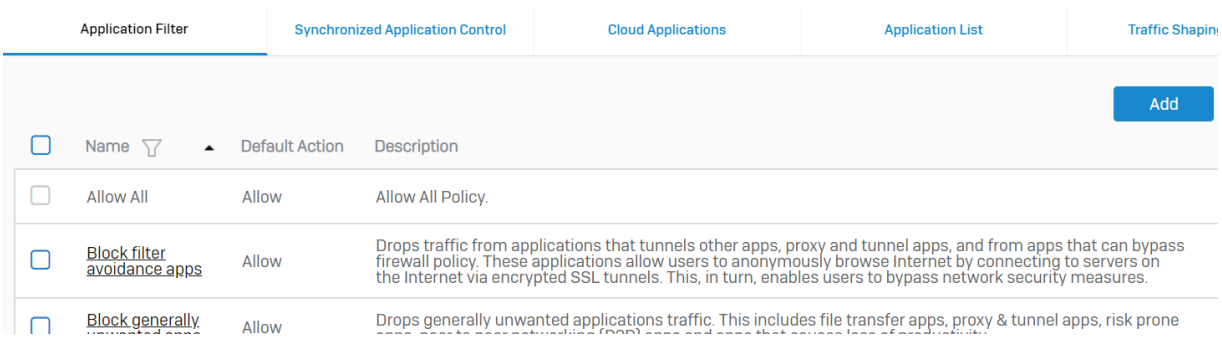
---

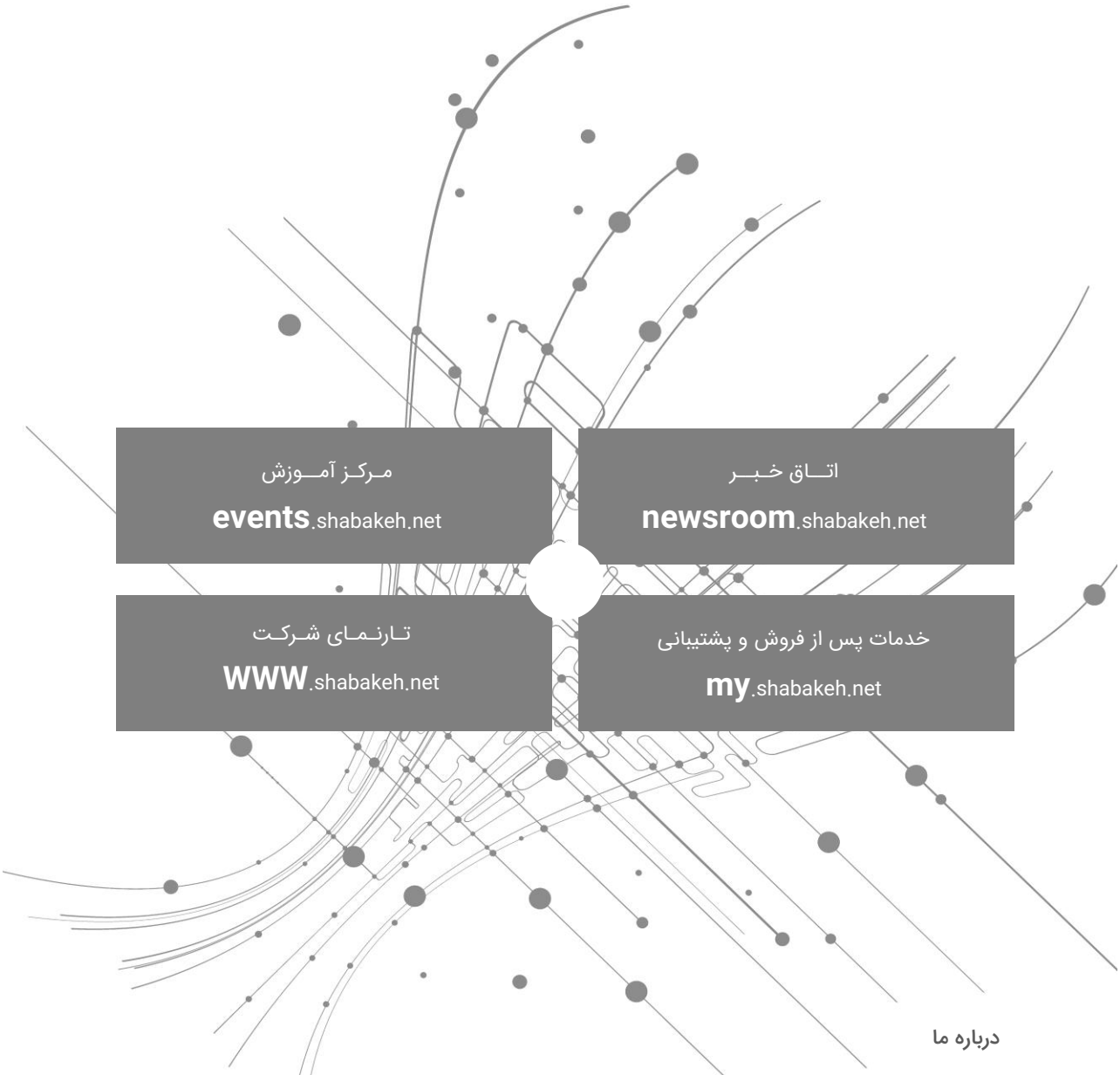
[۲] Complex Password
[۳] Character

جلوگیری از نشت اطلاعات سازمانی از طریق شبکه‌های اجتماعی

سرویس امنیتی Application Control در فایروال سوفوس امکان کنترل و مدیریت استفاده از شبکه‌های اجتماعی را فراهم می‌کند. در صورت نیاز برای جلوگیری از نشت اطلاعات از طریق این نوع برنامه‌ها، می‌توان با سرویس فوق، دسترسی به برنامه‌های مذکور را محدود کرد. تنظیمات مربوط به این سرویس امنیتی در صفحه Application Filter از منوی Protect > Applications قابل دسترس می‌باشد.







درباره ما

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تاسیس شد. این شرکت یکی از باسابقه‌ترین شرکتهای فعال در حوزه امنیت فناوری اطلاعات است. با بیش از ۲۵ سال تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدمات‌دهی به هزاران شرکت و سازمان در بخش‌های مختلف کشور را دارد و مجری بزرگترین پروژه‌های نصب و نگهداری نرم‌افزارهای ضدبدافزار و سخت‌افزارهای دیـواره آتش در کشور بوده است.

شبکه گستر
شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران خیابان شهید دستگردی (ظـفـر) شماره ۲۷۳
تلفن / دورنگار ۴۲۰۵۲ – ۰۲۱
info@shabakeh.net www.shabakeh.net