

SOPHOS

Cybersecurity made simple.

راهنمای مقاومسازی محصولات Sophos XG Firewall

بر اساس توصیه‌نامه مرکز ماهر

شبکه‌گستر

امنیت شما | وظیفه ما

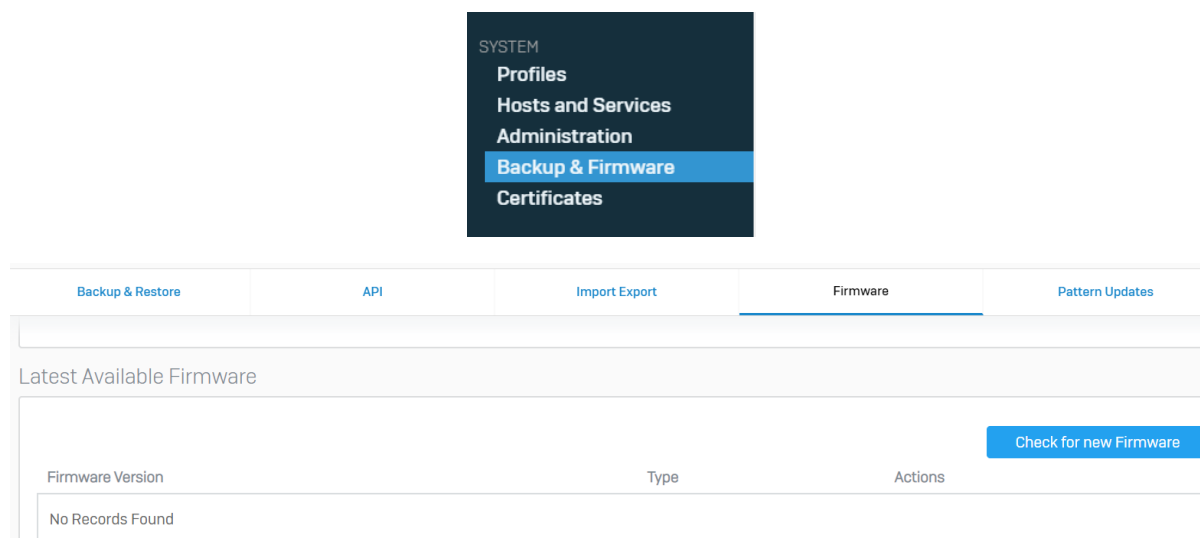
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) توصیه‌نامه‌ای برای امن‌سازی سامانه‌های فناوری اطلاعات در مقابل تهدیدات سایبری احتمالی همزمان با ۱۳ آبان ماه منتشر کرده که در آن طی ۱۰ بند مواردی جهت مقاوم‌سازی سامانه‌ها ارائه شده است.

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

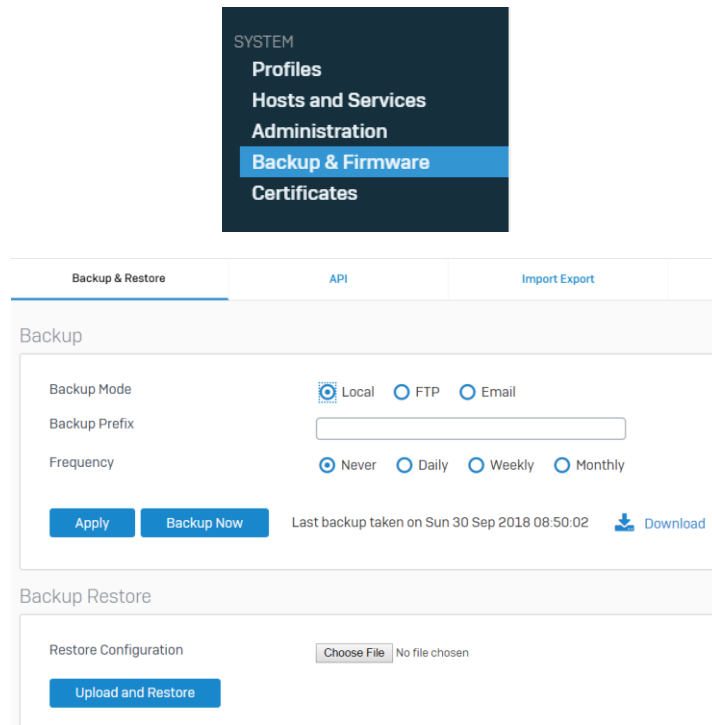
فایروال سوفوس تنها برند فایروال معتبر جهانی است که به‌روزرسانی آن برای نشانی‌های IP ایران هیچ محدودیتی ندارد و بطور مستقیم و برخط انجام می‌شود. برای اطمینان از به‌روز بودن ثابت‌افزار و داده‌های امنیتی فایروال می‌توان در منوی System > Backup & Firmware در کنسول تحت وب دستگاه به صفحات Firmware و Pattern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



The screenshot displays the Sophos XG Firewall management interface. On the left, a dark sidebar menu lists 'SYSTEM' categories: Profiles, Hosts and Services, Administration, Backup & Firmware (highlighted in blue), and Certificates. The main content area shows a navigation bar with tabs: Backup & Restore, API, Import Export, Firmware (selected), and Pattern Updates. Below the navigation bar, the 'Latest Available Firmware' section is visible, featuring a 'Check for new Firmware' button and a table with columns for Firmware Version, Type, and Actions. The table currently shows 'No Records Found'.

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.

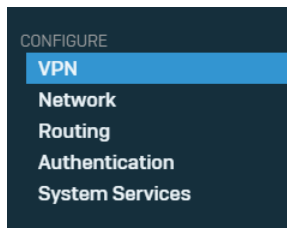


بهره‌گیری از رمزنگاری مناسب در تبادل اطلاعات

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 VPN > Configure مراجعه کرد.



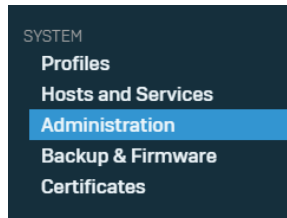
IPsec Connections

Show additional properties Add Delete Wizard

Name	Group Name	Policy	Connection Type	Status	Manage
No Records Found					

اتخاذ راه حل برای دسترسی ایمن از راه دور برای مدیریت سرویس ها و زیرساخت ها

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



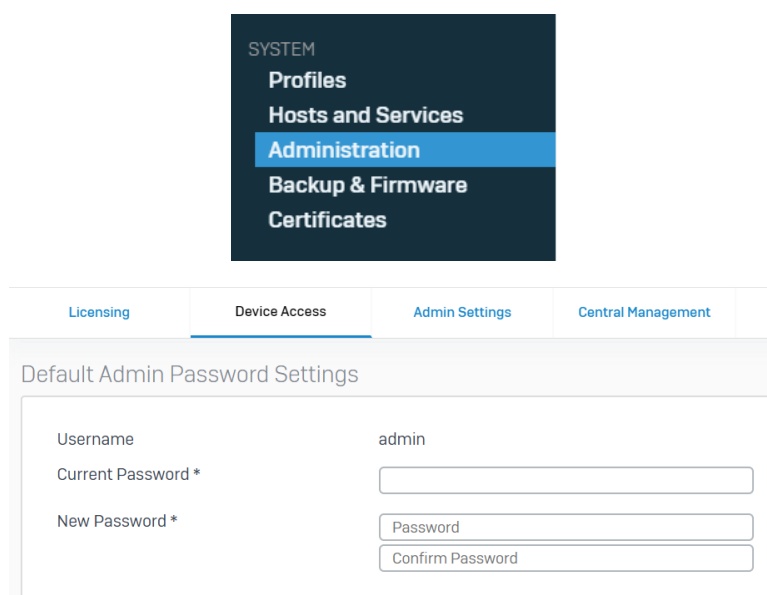
Licensing Device Access Admin Settings Central Management Time Notification Settings SNMP

Local Service ACL

Zone	Admin Services		Authentication Services					Network Services		Other Services						
	HTTPS	Telnet	SSH	NTLM	Captive Portal	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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.



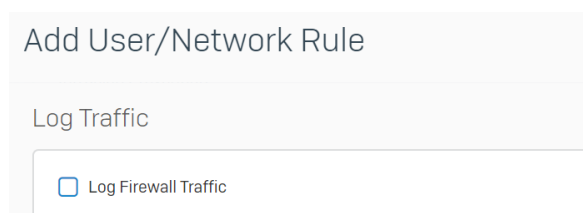
The screenshot shows the 'Administration' menu in the Sophos XG interface. The 'Device Access' tab is selected, leading to the 'Default Admin Password Settings' page. The form contains the following fields:

Field	Value
Username	admin
Current Password *	[Empty field]
New Password *	Password
	Confirm Password

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.

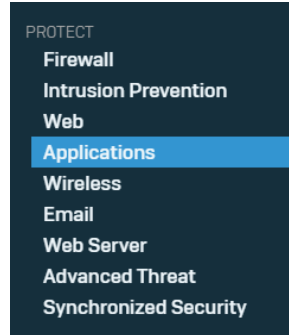


The screenshot shows the 'Add User/Network Rule' dialog box. Under the 'Log Traffic' section, the 'Log Firewall Traffic' checkbox is checked.

Complex Password^۲
Character^۳

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.



Application Filter	Synchronized Application Control	Cloud Applications	Application List	Traffic Shaping	
Add					
<input type="checkbox"/>	Name	▼	▲	Default Action	Description
<input type="checkbox"/>	Allow All			Allow	Allow All Policy.
<input type="checkbox"/>	Block filter avoidance apps			Allow	Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.
<input type="checkbox"/>	Block generally unwanted apps			Allow	Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, remote desktop (RDP) apps and apps that cause loss of productivity.

مرکز آموزش

events.shabakeh.net

اتاق خبر

newsroom.shabakeh.net

تارنمای شرکت

www.shabakeh.net

خدمات پس از فروش و پشتیبانی

my.shabakeh.net

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 دیواره آتش در کشور بوده است.

تهران خیابان شهید دستگردی (ظفر) شماره ۲۲۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

www.shabakeh.net info@shabakeh.net

شبکه گستر

شرکت مهندسی شبکه گستر