عنوان سند: چک لیست ممیزی امنیتی و مقاوم سازی فایروال Fortigate	کارفرما: گروه امنیت سازمان	تاریخ تهیه سند: ۱۴۰۱/۱۰/۱۵
	پیمانکار: شرکت فناوری اطلاعات	سرممیز و مدرس دوره : سیدحسام الدین حسینی

کنترل امنیتی	پاسخ			توضیحات	دلایل امنیتی (کنترل امنیتی تبعات مثبت و منفی اعمال)	نحوه ممیزی	اقدام اصلاحی
	بلی	خیر	نامربوط				
آیا برای فرآیند رمزنگاری فایل پیکربندی، از private key سازمان استفاده شده است؟				در حال پیش فرض برای رمزنگاری فایل پیکربندی از Private key پیش فرض خود تجهیز استفاده میشود که پیشنهاد میشود یک Private key برای سازمان به منظور فرآیند رمزنگاری تعیین گردد		#show system global	#Config system global set private-data-encryption enable
آیا ملاحظات فعال یا غیرفعال کردن اکانت Maintainer رعایت شده است؟				اکانت Maintainer بمنظور ریکاوری پسورد مورد استفاده قرار میگیرد که اگر در سازمان مورد استفاده قرار نمیگیرد بایستی غیرفعال شود.	اگر اکانت فعال باشد امکان سوء استفاده از این اکانت با ریبوت کردن تجهیز و ریست کردن پسورد ادمین وجود دارد. اگر اکانت غیرفعال باشد در صورت فراموش کردن پسورد ادمین، امکان ریکاوری پسورد وجود نخواهد شد و دستگاه باید به حالت پیش فرض کارخانه برگردد. پیشنهاد میشود نسبت به رعایت ملاحظات دسترسی فیزیکی و ساخت حداقل ۲ اکانت با سطح دسترسی ادمین اقدام گردد.	#show system global	#config system global set admin-maintainer disable
آیا پروتکل های نا امن مانند HTTP, Telnet غیرفعال شده است؟				پروتکل های Telnet و HTTP ارتباط بدون رمزنگاری دارد و باید با پروتکل های امن SSH و HTTPS جایگزین شود	استفاده از پروتکل های نا امن و Clear Text موجب حملات Sniffing و MITM خواهد بود.	#show system global	#config system global set admin-telnet disable
آیا سرویس های HTTPS, SSH فقط بر روی اینترفیس MGMT فعال شده است؟				دسترسی به تجهیز از طریق پروتکل های SSH و HTTPS فقط باید روی اینترفیس مدیریتی تجهیز (Management) فعال شود و روی سایر اینترفیس ها غیرفعال شود.	این پروتکل ها فقط بایستی روی اینترفیس مدیریتی (MGMT) فعال باشد فعال بودن این پروتکل ها روی سایر اینترفیس ها ضرورتی نداشته و موجب باز شدن پورت و حمله به تجهیز خواهد شد.	#show system interface	#config system interface edit MGMT set allowaccess https ssh
آیا سرویس SCP جهت کپی به روش امن فعال شده است؟				جهت کپی فریم ویر به تجهیز و یا کپی کانفیگ از روی تجهیز به سرور بایستی از روش کپی امن به همراه رمزنگاری توسط پروتکل SCP انجام گیرد.	استفاده از پروتکل های نا امن و Clear Text موجب حملات Sniffing و MITM خواهد بود.	#show system global	#config system global set admin-scp enable
آیا سرویس های HTTPS, SSH, Ping, ... بر روی کلیه اینتفریس های DMZ, WAN, LAN غیرفعال شده است؟				کلیه پروتکل های SSH, HTTPS, SNMP ,Ping, ... بر روی کلیه اینترفیس های فایروال بایستی غیرفعال گردد.	این پروتکل ها فقط بایستی روی اینترفیس مدیریتی (MGMT) فعال باشد فعال بودن این پروتکل ها روی سایر اینترفیس ها ضرورتی نداشته و موجب باز شدن پورت و حمله به تجهیز خواهد شد.	#show system interface	#config system interface edit WAN unset allowaccess edit DMZ unset allowaccess edit LAN unset allowaccess
آیا آخرین نسخه از FortiOS بر روی تجهیز نصب شده است؟				آخرین نسخه پایدار سیستم عامل FortiOS از وب سایت شرکت بایستی دانلود و نصب گردد.	بایستی قرارداد فعال با پیمانکار در خصوص به روز رسانی سیستم عامل بصورت دوره ای وجود داشته باشد.	#get system status	#execute restore image tftp <filename> <tftp_ipv4>
آیا TLS 1.2 برای ارتباط HTTPS با تجهیز پیکربندی شده است؟				برای تامین امنیت بیشتر ارتباط Https با تجهیز پیشنهاد میشود از TLS نسخه ۱,۲ استفاده گردد		#show system global	#config system global set admin-https-ssl-versions tlsv1-2
آیا درخواستهای HTTP به HTTPS هدایت خواهد شد؟				درخواستهای HTTP جهت مدیریت تجهیز بصورت وب بیس بایستی به HTTPS انتقال داده شود.		#show system global	#config system global set admin-https-redirect enable
آیا پورت های استاندارد مربوط به HTTPS و SSH تغییر کرده است؟				پورتهای پیش فرض SSH و HTTPS بایستی به شماره پروتهای ناشناس تغییر کند	استفاده از پورتهای شناخته شده، شرایط حمله به تجهیز را برای مهاجم تسهیل می کند	#show system global	#config system global set admin-sport 7734 set admin-ssh-port 2345
آیا قطع ارتباط در صورت مدت زمان بیکاری پیکربندی شده است؟				در صورتی که ارتباط با تجهیز برای مدت زمان مشخصی بیکار باشد باید ارتباط قطع شود		#show system global	#config system global set admintimeout 5
آیا مدت زمان بین ارتباط SSH و لاگین به تجهیز محدود شده است؟				از زمانی که ارتباط SSH برقرار میشود اگر مدت زمان مشخصی بگذرد و ادمین لاگین موفق به تجهیز نداشته باشد ارتباط قطع شود (جلوگیری از حمله Brute Force)	در صورت عدم پیکربندی این کنترل، شرایط حمله Brute Force برای مهاجم تسهیل خواهد شد	#show system global	#config system global set admin-ssh-grace-time 30
آیا امکان لاگین به تجهیز محدود به سیستم ادمین شبکه شده است؟				امکان اتصال و لاگین به تجهیز فایروال باید محدود به آدرس IP سیستم ادمین شبکه باشد.		#show system admin	#config system admin edit set trustedhost1 172.25.176.23 255.255.255.255
آیا برای ادمین های مختلف ، اکانت اختصاصی ایجاد شده است؟				برای ادمین های مختلف بایستی اکانت اختصاصی ایجاد شود و از اکانت Admin بصورت اشتراکی استفاده نشود		#show system admin	#config system admin edit <admin_name> set accprofile "super_admin" set vdom "root" set passwor <password for this admin>
آیا تعداد تلاش ناموفق جهت لاگین به تجهیز محدود شده است؟				تعداد تلاش ناموفق جهت لاگین به تجهیز باید محدود شود (جلوگیری از حمله Brute Force)	در صورت عدم پیکربندی این کنترل، شرایط حمله Brute Force برای مهاجم تسهیل خواهد شد	#show system global	#config system global set admin-lockout-threshold 3
آیا در صورت تعداد مشخص لاگین ناموفق اکانت غیرفعال خواهد شد؟				در صورتی که تعداد مشخصی لاگین ناموفق صورت گرفت اکانت کاربر باید برای مدت مشخصی غیرفعال شود.	در صورت عدم پیکربندی این کنترل، شرایط حمله Brute Force برای مهاجم تسهیل خواهد شد	#show system global	#config system global set admin-lockout-duration 300
آیا اکانت Admin تغییر نام داده شده است؟				اکانت پیش فرض Admin بایستی غیرفعال و یا تغییر نام داده شود (جلوگیری از حمله Brute Force)	در صورت عدم تغییر نام اکانت Admin شرایط حمله Force Brute برای مهاجم تسهیل خواهد شد	#show system admin	#config system admin edit rename admin to manager