بسمه تعالی

مرکز مدیریت راهبردی افتا

عنوان

پیشنهادات امنیتی برای امن‌سازی زیرساخت شبکه

گروه زیر ساخت امن

تیرماه ۱۳۹۳

۱. مقدمه

در سالهای اخیر بسیاری از شبکه‌ها در سازمان‌ها و شرکت‌های خصوصی و دولتی مورد نفوذهای بی‌شماری قرار گرفته‌اند که موجب سوء استفاده‌های سایبری شده است. تهدیدات مربوط به شبکه و سیستم‌های موجود بین قسمت‌های مختلف همچون تجهیزات کاربر نهایی، سرورها و تجهیزات زیر ساخت شبکه می‌باشد. به این منظور این بخشنامه جهت مقاوم‌سازی شبکه در قبال تهدیدات منتشر شده است.
قبل از مطالعه و اجرای این سند، نکات زیر باید مورد توجه قرار گیرد:

- از آن‌جا که ممکن است تنظیمات امن‌سازی، کارکردهای سیستم را مختل یا غیرفعال کند، لازم است قبل از اجرای تنظیمات، یک نسخه پشتیبان از پیکربندی سیستم تهیه شود.
- برای اجرای الزامات تعیین شده در این سند، اولویت با خط‌مشی‌های سازمان است. به عبارت دیگر اگر برخی از الزامات بیان شده در این سند، با خط‌مشی‌های سازمان تداخل یا تضاد داشت، اولویت با خط‌مشی‌های سازمان است.
- در تهیه این سند، سعی شده است که حداکثر الزامات مرتبط با حوزه‌ی سند، پوشش داده شود. اما این بدان معنا نیست که پس از اجرای این الزامات، سیستم به صورت صد در صد امن خواهد بود. الزامات بیان شده در این سند، حداقل انتظارات برای امن‌سازی در حوزه‌ی تعریف شده در این مستند است.

۱,۱ تهدیدات

خطرات خاصی که ممکن است اتفاق بیفتد اگر امنیت زیرساخت شبکه به خوبی مدیریت نشود شامل موارد زیر می‌شود:

۱,۱,۱ از دست رفتن محرمانگی[۱] اطلاعات

[۱] Confidentiality

داده منتقل شده روی شبکه در معرض خطر استراق سمع توسط یک بخش غیرمجاز می‌باشد. علاوه بر آن، کنترل ضعیف روی دسترسی به شبکه ممکن است سبب ذخیره‌ی داده روی کارگزار[۲] یا ایستگاه‌های کاری[۳] که در معرض دسترسی غیرمجاز[۴] هستند، شود.

۲،۱،۱ از دست رفتن صحت[۵] اطلاعات

داده ممکن است در حین انتقال بین گره‌های شبکه به صورت عمدی یا سهوا تغییر داده شود. این اتفاق ممکن است منجر به ایجاد خطا در فرایند سامانه‌ی[۶] دریافت یا داده‌ی مخرب شود.

۳،۱،۱ منع خدمت[۷]

یک سامانه متصل به شبکه، بر عملکرد همه‌ی لینک‌های شبکه متکی می‌باشد. حال قطع یا کاهش سرعت یک لینک شبکه ممکن است از فراهم آوردن خدمات لازم توسط سامانه جلوگیری کند.

۴،۱،۱ لورفتن[۸] سامانه

سامانه‌های متصل به شبکه شامل مسیریاب‌ها، کارگزارهای DNS[۹]، مودم‌ها و دیگر ادوات اتصال، در معرض خطر لورفتن قرار دارند و منابعشان برای اهداف غیرمشروع مانند حمله‌ی منع خدمت، سرقت پهنای باند یا تشدید تسخیر سامانه بکار برده می‌شود.

---

۲ Server
۳ WorkStation
۴ Unauthorized
۵ Integrity
۶ System
۷ Denial of Service
۸ Compromise
۹ Domain Name System

۲,۱ دامنه

در این متن هدف بررسی تهدیدات موجود بر روی زیرساخت شبکه و ارائه پیشنهاداتی جهت امن‌سازی این زیرساخت می‌باشد. در این راستا پیشنهادات امنیتی کلان و اجرایی که شامل امنیت اتصالات شبکه‌ی داخلی و خارجی می‌باشد ارائه شده است.

۳,۱ اصطلاحات

۱,۳,۱ خطایابی ونگهداری غیرمحلی(Non-local maintenance & diagnostic session)

فعالیت‌های خطایابی و نگهداری غیرمحلی آن دسته از فعالیت‌هایی هستند که توسط ارتباطات مجزا از طریق یک شبکه (شبکه خارجی مثل اینترنت یا یک شبکه داخلی) انجام می‌شود.

۲,۳,۱ خطایابی ونگهداری محلی(Local maintenance & diagnostic session)

فعالیت‌های خطایابی و نگهداری محلی آن دسته از فعالیت‌ها هستند که توسط بخش‌های فیزیکی مجزا که در یک سامانه اطلاعاتی وجود دارند، انجام می‌شود و نه در ارتباطاتی که در سطح شبکه صورت می‌گیرد.

۳,۳,۱ Dual authorization (مجازشناسی دوگانه)

هرگونه تغییری که توسط سرپرست در پیکربندی صورت گیرد، تنها پس از تائید توسط سرپرست دیگر فعال می‌شود.

۴,۳,۱ Boundary protection(حفاظت مرزی)

نظارت و کنترل ارتباطات بین مرزهای خارجی بین یک سامانه‌ی اطلاعاتی داخل سازمان، و یک سامانه‌ی اطلاعاتی خارجی، یا بین مرزهای حساس بین سامانه‌های اطلاعاتی داخلی برای جلوگیری و کشف ارتباطات مخرب و غیر مجاز، با استفاده از واسط‌های کنترلی مانند مسیریاب، دروازه، تونل رمز شده و غیره.

۵,۳,۱ Mobile code(کد سیار)

در علم کامپیوتر، کد سیار نرم‌افزاری است که بین سیستم‌ها منتقل می‌گردد؛ به عنوان مثال، بین شبکه منتقل می‌گردد و بدون نصب بر روی سیستم محلی اجرا می‌گردد.

۶,۳,۱ کد سیار ممنوع (Prohibited Mobile Code)

آن دسته از کدهایی که استفاده از آنها در سامانه اطلاعاتی با توجه به دستورالعمل‌ها ممنوع است. کد سیارهایی که ممنوع هستند شامل تمام کد سیارها در دسته 1X، دسته 1A و دسته ۲، تمام کدسیارهای فن‌آوری‌های در حال ظهور و تمام کد سیارهای که از طریق ایمیل یا پیوست ایمیل زمانیکه کاربر ایمیل را باز می‌کند به صورت خودکار اجرا می‌شوند.

۷,۳,۱ Safeguard (تدابیر حفاظتی)

هر معیار یا کنترل حفاظتی برای برآوردن نیازهای امنیتی یک سامانه‌ی اطلاعاتی مانند حفظ محرمانگی، تضمین صحت، و تداوم دسترس‌پذیری توصیه می‌شود. این نوع حفاظت‌ها می‌توانند ویژگی‌های امنیتی سخت-افزارها و نرم‌افزارها، رویه‌های اجرایی، شیوه‌های پاسخگویی، کنترل‌های دسترسی، محدودیت‌های مدیریتی، امنیت کارکنان، ساختارهای فیزیکی، نواحی، و تجهیزات سازمان را شامل شوند اما فقط به این موارد محدود نیست.

۸,۳,۱ False positive(مثبت غلط)

اخطاری که به نادرست انجام یک فعالیت بدخواهانه را اعلام می‌کند.

۹,۳,۱ احرازهویت چندفاکتوری (Multifactor authentication)

احراز هویت چندفاکتوری رویکردی است که جهت احرازهویت نمودن ملزم به ارائه‌ی دو یا بیش از سه فاکتور می‌باشد: «آنچه که کاربر می‌داند»، «آنچه که تنها کاربر دارد» و «آنچه که تنها متعلق به کاربر است».

۱۰,۳,۱ کنترل دسترسی اختیاری(DAC)[۱۰]

[۱۰] Discretionary Access Control

کنترل دسترسی مکانیزمی است که نحوه دسترسی کاربران به منابع سیستم را محدود به نیازهای آنها می‌نماید و به طریقی نحوه تامین امنیت داده‌ها و تنظیم حق دسترسی را بیان می‌دارد. مدل‌های کنترل دسترسی مختلفی وجود دارد، در مدل کنترل دسترسی اختیاری به هر کاربر اجازه داده می‌شود نحوه دسترسی به داده-های خود را تحت کنترل داشته باشد.

۲. امن‌سازی زیرساخت شبکه

در این بخش امن سازی زیرساخت شبکه مورد بحث قرار می‌گیرد. این بخش شامل دو زیر بخش است. در زیربخش اول امن سازی زیرساخت بصورت کلان و فارغ از نوع شبکه و تجهیزات بحث خواهد شد و در زیربخش دوم امن سازی در سطح اجرای زیرساخت مورد بحث قرار می گیرد.

۱,۲ امن سازی کلان زیرساخت شبکه

در سطح کلان امن‌سازی زیر ساخت شبکه در چهار بخش زیر مطرح شده است:

۱,۱,۲ صحت و یکپارچگی تجهیزات

- برای تضمین صحت تجهیزات لازم است تا تجهیزات شبکه تنها از تولید کننده یا از فروشندگانی که توسط تولید کننده تجهیزات مجاز و تائید شده‌اند، خریداری گردد.
- باید پیش از نصب میان افزار [۱۱] و یا سیستم عامل جدید بر روی تجهیزات شبکه، با مقایسه کد درهمسازی میان افزار تجهیزات شبکه با کد درهمسازی که تولید کننده منتشر نموده، از صحت آن اطمینان ایجاد نمود و باید از نصب و اجرای نسخه‌هایی از میان افزار تجهیزات شبکه که تولید کننده در دسترس قرار نداده، جلوگیری گردد.
- بر روی شبکه، واسط‌های فیزیکی که بر روی تجهیزات شبکه استفاده نمی‌شوند باید خاموش یا غیر فعال گردند.

---

[۱۱] Firmware

- با ایجاد لیست دسترسی که تنها دسترسی پورت‌ها، پروتکل‌ها و آدرس‌های IP که کاربران شبکه و سرویس‌ها به آنها نیاز دارند، مجاز می‌کند، و هرچیزی جز موارد ذکر شده در لیست رد می‌شود، دسترسی به تجهیزات محدود شود.
- همچنین سرویس‌های غیر ضروری بر روی تجهیزات شبکه باید خاموش شوند.
- از افشاء غیرمجاز فایل‌های پیکربندی تجهیزات شبکه باید محافظت گردد، بدین منظور باید مراحلی در نظر گرفته شود که از ظاهر شدن کلمه عبور به صورت آشکار (بدون آنکه رمز شود) جلوگیری نماید. استفاده نمودن از رمزنگاری یا درهمسازی با تکرار جهت حفاظت از محرمانگی کلمه عبور در فایل‌های پیکربندی لازم و ضروری می‌باشد، لازم به ذکر است کدگذاری به تنهایی کافی نیست.
- در صورتی‌که فایل پیکربندی تجهیزات شبکه به صورت آشکار منتقل شود و در برگیرنده‌ی کلیدها/کلمه عبورهای رمز نشده باشد، بلافاصله باید کلمه عبورها/کلیدها را تغییر داد.
- از پروتکل‌های امن هنگام انتقال فایل‌های پیکربندی تجهیزات شبکه باید استفاده گردد.
- باید از تولید رویدادهای ممیزی در هنگام راه‌اندازی مجدد و اعمال تغییرات پیکربندی به تجهیزات شبکه اطمینان یافت.
- گزارش‌های شبکه باید به صورت دوره‌ای بررسی شوند تا فهم عمیقی نسب به رفتار شبکه نرمال حاصل شود.

۲,۱,۲ مدیریت امن

- سند کتبی خطمشی امنیتی زیر ساخت شبکه باید ایجاد و نگهداری شود. این سند باید مشخص نماید که چه افرادی مجاز به ورود تجهیزات زیرساخت شبکه هستند و چه کسی مجاز به پیکربندی تجهیزات شبکه می‌باشد، همچنین باید طرحی را برای بروزرسانی میان افزار تجهیزات شبکه در فواصل زمانی مشخص تعریف نماید.
- از نام‌های کاربری و کلمه‌عبورهای متداول نباید استفاده شود. خطمشی زیرساخت شبکه باید الزاماتی بر روی طول کلمه عبور و پیچیدگی آن تعریف نماید.
- تنها از استانداردهای پروتکل امن در زمان مدیریت نمودن از راه دور تجهیزرات شبکه باید استفاده شود. برای آگاهی بیشتر به پیوست الف از سند پروفایل حفاظتی تجهیزات شبکه مراجعه شود.

- اتصالات مدیریت از راه دور باید تنها به ماشین‌های کنترل شده‌ای محدود گردد که بر روی یک دامین امنیتی مجزا با حفاظت قوی هستند.
- از حداقل دو NTP تائید شده برای حفظ یک زمان ثابت بین تجهیزات شبکه باید استفاده شود.

۳,۱,۲ استانداردهای پروتکل امن و رمزنگاری قوی

- در بحث امنیت زیر ساخت شبکه باید از پروتکل‌ها و الگوریتم‌هایی استفاده شود که مورد تائید باشند.
- در هنگام مدیریت از راه دور تجهیزات شبکه باید از راهنمای استاندارد NIST SP 800-131A برای الگوریتم‌های رمزنگاری و اندازه کلید تبعیت گردد.
- هنگام استفاده از پروتکل SNMP، باید از SNMP v3 با فعال نمودن رمزنگاری استفاده شود و/یا تمام ترافیک شبکه در یک تونل IPsec کپسوله گردد.
- تمام VPN های IPsec باید مطابق با استاندارد های IETF و راهنمای NIST SP 800-131A باشند. و در صورت امکان استانداردهای پروتکل امن IETF بکار برده شود.
- با استناد به استاندارد FIPS 140، باید موتور (یا هسته) رمزنگاری در تجهیزات شبکه مورد ارزیابی قرار گیرد، و الگوریتم‌های انتخاب شده‌ای که با توجه به ارزیابی پروفایل حفاظتی تجهیزات شبکه معتبر گردیده‌اند، پیکربندی گردد.

۴,۱,۲ رویدادنگاری امن[۱۲]

- از رویدادنگاری به منظور ردیابی اطلاعات امنیتی در سامانه یا زیرساخت شبکه استفاده می‌شود.
- برای رویدادنگاری امن باید از سرور ممیزی از راه دور (همانند Syslog server) استفاده شود. از محرمانگی و صحت و یکپارچگی داده‌های ممیزی باید با برقراری یک اتصال امن مانند IPsec VPN بین تجهیزات حساس شبکه و سرور ممیزی محافظت گردد.
- باید اطمینان حاصل گردد که تمام تجهیزات زیرساخت شبکه در زمان اعمال تغییرات پیکربندی، بروزرسانی میان افزار سیستم عامل و همچنین در زمان راه اندازی مجدد تجهیزات، رویداد ممیزی تولید می‌نمایند.
- باید اطمینان حاصل گردد که گزارش‌ها به صورت منظم بررسی می‌گردند.

---

[۱۲] Secure Logging

۲,۲ امن سازی اجرایی زیرساخت شبکه

از نظر اجرایی امن سازی شبکه، نیازهای اساسی جهت فراهم آمدن اصول امنیتی زیر ساخت شبکه به صورت زیر لیست شده است:

- تجهیزات شبکه باید به صورت امن پیکربندی و با یک روش امن قابل دسترسی باشند.
- پروتکل‌های امن باید برای ارتباطات شبکه بکار برده شود.
- شبکه‌های داخلی و خارجی باید به طور مناسبی از طریق استفاده از مناطق حائل (DMZ[۱۳]) و تجهیزات کنترلی (مثل دیواره‌های آتش[۱۴] به صورت امن پیکربندی شده یا جداول کنترل دسترسی مسیریاب)، از یکدیگر جداسازی شوند.
- دسترسی از راه دور[۱۵] به شبکه‌های داخلی باید به صورت امن مدیریت شود.
- شبکه‌های داخلی باید جهت جلوگیری یا تشخیص مبادرت به برقراری اتصال غیرمجاز و جریان یافتن ترافیک مشکوک، پیکربندی شوند.

۱,۲,۲ امن سازی ساختار شبکه‌ی داخلی

۱,۱,۲,۲ امنیت خدمات شبکه

مشخصات و مفاهیم امنیتی خدمات شبکه (قبل از اینکه قادر به استفاده در شبکه‌ها باشند) که باید در نظر گرفته شوند عبارتند از:

- مدیریت اتصال به خدمات شبکه. اتصال به یا از شبکه‌های خارجی باید شامل استفاده از خدمات شبکه-ی امن باشد.
- از آنجایی که داده‌های مربوط به خدمات شبکه ذاتا مهم و حساس هستند باید جهت جلوگیری از به خطر افتادن به وسیله‌ی اشخاص ثالث، رمزگذاری شوند (برای مثال از طریق بکارگیری خدمات شبکه‌ی امن مانند SSH برای نشست‌های انتهایی[۱۶] و SSL برای تبادل اطلاعات با وب‌سایت‌ها).

---

[۱۳] Demilitarized Zone

[۱۴] Firewalls

[۱۵] Remote Access

[۱۶] Terminal Session

۲,۱,۲,۲ ذخیره‌ی اطلاعات مهم روی سامانه‌های متصل به شبکه

اطلاعاتی مانند اطلاعات مالی نباید روی سامانه‌هایی که یا به شبکه‌های دشمن متصل هستند یا به طور مستقیم از آن‌ها قابل دسترس هستند (مثل اینترنت) ذخیره شوند. به طور مشابه، پایگاه داده و کارگزارهای دیگر که چنین اطلاعاتی را ذخیره می‌کنند نباید به طور مستقیم قابل دسترس از اینترنت باشند. استفاده از مناطق امنیتی شبکه به پیاده‌سازی این دستورالعمل کمک می‌کند.

۳,۱,۲,۲ کنترل اتصال به شبکه

نیاز است قابلیت اتصال کاربران به شبکه‌ها از طریق روش‌هایی مانند محدود کردن دسترسی شبکه به کاربران خاص در طول زمان‌های معین از روز یا هفته، تا جای ممکن محدود شود؛ به طور مثال اجازه‌ی انتقال فایل به کاربران فقط به صورت یکطرفه داده شود به طوریکه کاربران نتوانند فایل‌های مخرب را به شبکه بارگذاری کنند؛ و یا از VLANها جهت تسهیل در جداسازی تجهیزات و میزبان‌های[۱۷] شبکه (خصوصا پایگاه‌های داده و کارگزارها) استفاده شود به طوریکه جهت اطمینان از توانایی دسترسی پایگاه‌های داده فقط به خدمات شبکه‌ای که آن‌ها برای اهداف تجاری نیاز دارند، خط‌مشی‌های فیلتر کردن یکسان بکار برده شود. مثال‌هایی از خط‌مشی-های فیلتر کردن خوب عبارتند از:

- پایگاه‌های داده و کارگزارها هیچ‌کدام نمی‌توانند مستقیما به اینترنت وصل شوند. اتصال به اینترنت باید از طریق استفاده از یک پیشکار[۱۸] صورت بگیرد.
- همه‌ی پایگاه‌های داده می‌توانند به کارگزارهای مناسب (مانند کارگزارهای فایل، پرینت، پست الکترونیک[۱۹] و کاربرد) موردنیاز جهت قابلیت‌های مناسب متصل شوند. اگر کنترل دسترسی به منابع نیاز شود، از طریق استفاده از یک اکتیو دایرکتوری[۲۰] یا برپایی احراز هویت[۲۱] پیاده می‌شود.
- همه‌ی پایگاه‌های داده داخل یک بخش[۲۲] شبکه می‌توانند با استفاده از درگاه‌های[۲۳] شبکه‌ی مناسب به پیشکار به کار رفته در آن بخش وصل شوند.

---

[۱۷] Hosts
[۱۸] Proxy Server
[۱۹] Email
[۲۰] Active Directory
[۲۱] Authentication
[۲۲] Segment
[۲۳] Port

- همه‌ی پایگاه‌های داده متصل شده به بخش‌های شبکه که به احرازهویت نیاز دارند می‌توانند به منظور احرازهویت کاربر به سامانه‌های خدمات احرازهویت مهمان متصل شوند.
- جهت کنترل دسترسی پایگاه‌های داده به کارگزارها، لازم است از فیلتر کردن IPsec استفاده شود.

۴,۱,۲,۲ خدمات راهبری[۲۴]

دسترسی خدمات راهبری به سامانه‌ها و ادوات، به آدرس‌های IP داخلی مجاز محدود می‌شود. آدرس‌های IP داخلی مجاز برای مثال می‌توانند شامل مدیران IT یا راهبران سامانه، شبکه و پایگاه داده باشند.

۵,۱,۲,۲ محیط‌های توسعه و تست شبکه‌ها

محیط‌های توسعه و تست به منظور جلوگیری از دست رفتن اطلاعات و خطای دسترسی، به شبکه‌های منطقی[۲۵] جداگانه تقسیم می‌شوند.

محیط‌های توسعه به سامانه‌های شبکه‌ای اشاره دارد که تحت توسعه‌ی فعال هستند و به طور متوالی تغییر می‌کنند. محیط‌های تست به سامانه‌های شبکه یا سامانه‌های پایدار جهت تست اشاره دارد. جهت پیاده‌سازی مناسب این محیط‌ها باید به صورت زیر عمل شود:

- لازم است دسترسی از سامانه‌ها و محیط‌های تست و توسعه به سامانه‌ها یا محیط‌های محصولات تا حداقل میزان لازم محدود شود. این امر می‌تواند از طریق استفاده از VLANها یا دیگر مکانیزم‌های کنترل دسترسی مانند دیواره‌های آتش بدست آید.
- داده‌های تولید نباید از محیط‌های تست و توسعه بگذرد مگر اینکه کاملا نیاز باشد. اگر این داده‌ها در محیط تست و توسعه بکار برده شوند باید تحت کنترل‌های امنیتی قرار بگیرند.
- دسترسی به شبکه‌های تست و توسعه باید به کاربران مجاز محدود شود.
- محیط‌های در حال تست ممکن است به اجزاء محیط‌های توسعه دسترسی داشته باشند اما این دسترسی باید به حداقل دسترسی موردنیاز جهت تکمیل فرایند تست محدود گردد.

---

[۲۴] Administrative

[۲۵] Logical

۶,۱,۲,۲ دسترسی مهمان[۲۶]

ممکن است جهت دسترسی به منابعی خاص (مثل اینترنت)، شبکه‌های اختصاصی در دسترس مهمانان قرار گیرند. ولی این موضوع نباید امکان دسترسی مهمان به تنظیمات شبکه و نهایتا دسترسی به شبکه‌ی داخلی را فراهم کند.

لازم است پورتال کپتیو[۲۷] در محل شبکه‌های مهمان گذارده شود تا مهمانان مجبور به پذیرش شرایط گذاشته شده جهت استفاده‌ی قابل قبول بشوند. وقتی مهمانان این شرایط را قبول کردند آن‌ها تنها باید به شبکه‌های خارجی که برای اهداف تجاری نیاز دارند دسترسی پیدا کنند (مهمانان لازم است به دسترسی به اینترنتی با پهنای باند و خدمت محدود، مقید شوند).

۷,۱,۲,۲ دسترسی به کاربردهای داخلی

زمانیکه لازم است برنامه‌ی کاربردی داخل یک مرکز در دسترس مراکز دیگر قرار بگیرد، این دسترسی باید از طریق استفاده از شبکه اختصاصی مجازی (VPN[۲۸]) و فقط بر اساس نیاز[۲۹] صورت بگیرد.

۲,۲,۲ دستورالعمل اتصال خارجی

[۲۶] Visitor
[۲۷] Captive Portal
[۲۸] Virtual Private Network
[۲۹] Need-basis

۱,۲,۲,۲ دسترسی شخص ثالث به شبکه‌های داخلی

دسترسی VPN یا dial up به شبکه‌ی داخلی به اشخاص ثالث داده نمی‌شود مگر به مدیر IT در هنگام نیاز قانونی. در عین حال اگر نیاز مشروع جهت دسترسی وجود داشت، دسترسی باید تنها برای دوره‌ی زمانی محدودی که شخص ثالث بتواند کارش را به اتمام برساند، داده شود.

۲,۲,۲,۲ احراز هویت کاربر برای اتصالات خارجی

دسترسی به داده، خدمات و برنامه‌های کاربردی خارج از دسترس میزبان از طریق اتصالات خارجی، باید فقط به کاربری که به عنوان کاربر مجاز شناسایی و احرازهویت شده باشد، اجازه داده شود. لازم به ذکر است نباید امکان گذشتن و دور زدن مرحله‌ی احراز هویت وجود داشته باشد.

قدرت سازوکار احراز هویت کاربر بکار برده شده به حساسیت اطلاعات بکار گرفته شده توسط شبکه بستگی دارد. سازوکار احراز هویت مناسب شامل موارد زیر می‌باشد اما به آن محدود نمی‌شود:

- توکن سخت افزاری
- تکنیک‌های رمزنگاشتی[۳۰]
- پروتکل‌های چالشی-پاسخی[۳۱]

هر کاربر جهت اتصال به شبکه‌ی اینترنت باید از طریق VPN متصل شود. چند تکنیک VPN در زیر آمده است:

- پروتکل L2TP[۳۲]
- IPsec
- لایه‌ی دریچه‌ی امن (SSL[۳۳]) با استفاده از حداقل رمزگذاری[۳۴] ۱۲۸ بیتی

---

[۳۰] Cryptographic
[۳۱] Challenge-response
[۳۲] Layer 2 Tunneling Protocol
[۳۳] Secure Socket Layer
[۳۴] Encryption

۳,۲,۲,۲ تفکیک اتصالات اینترنت

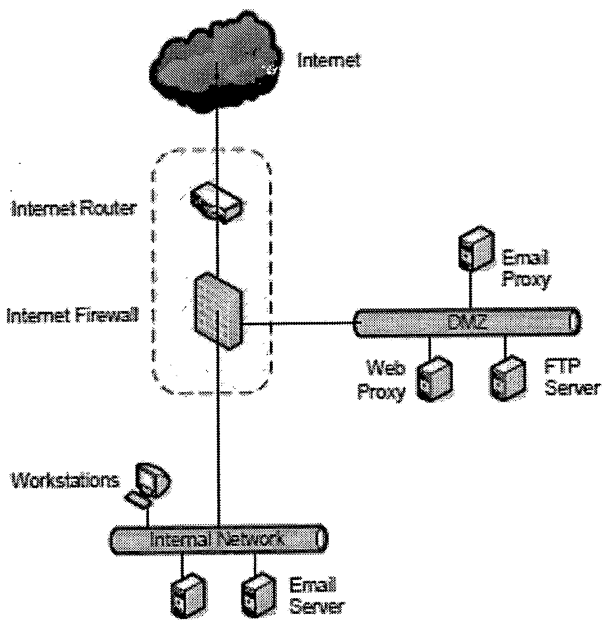
اتصالات اینترنت از دیگر شبکه‌های داخلی جدا شوند. اتصالات اینترنت به عنوان یک شبکه‌ی دشمن رفتار می‌کند. به منظور حمایت از شبکه‌های متصل شده به اینترنت، کنترل‌های زیر بهتر است رعایت شود:

- همه‌ی ترافیک‌های ورودی و خروجی از طریق دیواره‌ی آتش لایه‌ی انتقال یا تجهیزات معادل دیگر گذشته و به وسیله‌ی آن فیلتر می‌شوند. این دستگاه بعدا به عنوان دیواره‌ی آتش اینترنت[۳۵] یاد می‌شود.
- دیواره‌ی آتش اینترنت فقط اجازه‌ی دسترسی مجموعه‌ی کمی از انواع سرویس‌های موردنیاز جهت اهداف تجاری را، به و از سیستم‌های شبکه‌ی داخلی می‌دهد.
- شبکه‌های تولید، توسعه و تست به صورت فیزیکی جدا شده‌اند.

نمودار ۱ راه‌کار پیشنهادی جهت پیاده‌سازی ساختار اتصالات اینترنت را نشان می‌دهد.

توجه ۱: دیواره‌ی آتش اینترنت و دیواره‌ی آتش مسیریاب ممکن است در برخی سناریوها با هم ترکیب شده و به عنوان یک دستگاه در شکل نشان داده شوند. این بسته به نوع سرویس اینترنت و تکنولوژی ارتباطاتی بکار گرفته شده جهت خاتمه دادن به آن سرویس متفاوت است.

توجه ۲: پروکسی پست الکترونیک[۳۶] متفاوت از پروکسی وب[۳۷] عمل می‌کند و علاقه‌مند به انتقال ایمیل به/ از کارگزار ایمیل قرارگرفته در شبکه داخلی می‌باشد. علاوه بر این، این کارگزار به عنوان دسترسی مشتری برای تکنولوژی‌هایی مثل OWA[۳۸] و RPC[۳۹] روی http عمل می‌کند.



[۳۵] Internet Firewall
[۳۶] Email Proxy
[۳۷] Web Proxy
[۳۸] Outlook Web Access
[۳۹] Remote Procedure Calls

نمودار ۱. نمودار طراحی اتصال اینترنت

کنترل‌های بیشتر که بهتر است رعایت شوند:

- هیچ ترافیکی قادر به برقراری ارتباط بین سامانه‌های دارای ارتباطات اینترنتی و سامانه‌هایی بدون ارتباطات اینترنتی، بدون گذاشتن و فیلتر شدن بوسیله‌ی دیواره‌ی آتش لایه‌ی کاربرد یا تجهیزات معادل (مانند پروکسی[۴۰]) نیست. این تجهیزات دیواره‌ی آتش داخلی[۴۱] نامیده می‌شوند.
- هنگام پیاده‌سازی سامانه‌های دارای ارتباطات اینترنتی، همه‌ی آن‌ها در یک منطقه‌ی حائل که بوسیله‌ی دیواره‌ی آتش اینترنت تولید شده، قرار داده می‌شوند.
- دیواره‌ی آتش داخلی فقط اجازه‌ی دسترسی مجموعه‌ی کمی از انواع خدمات موردنیاز جهت اهداف تجاری را، به و از سامانه‌های موجود در منطقه‌ی حائل می‌دهد.
- همه‌ی سامانه‌های منطقه‌ی حائل نرم‌افزار آنتی ویروس را به‌صورت نصب شده دارا می‌باشند.

۴,۲,۲,۲ اتصالات بی‌سیم

اتصالات بی‌سیم از شبکه‌های داخلی سیمی از طریق حداقل یک نقطه‌ی کنترلی[۴۲] جدا شده‌اند.

هنگام پیاده‌سازی شبکه‌های بی‌سیم، حمایت از شبکه‌ی بی‌سیم، جهت اطمینان از حداقل شدن دسترسی غیرمجاز نیاز می‌باشد. در این راستا کنترل‌های زیر بهتر است رعایت شود:

- شبکه‌های بی‌سیم باید با استفاده از دیواره‌ی آتش لایه‌ی انتقال به‌طور فیزیکی از شبکه‌های دیگر جدا شود.
- گره‌های گیرنده و فرستنده یک شبکه‌ی بی‌سیم به صورت دو به دو همدیگر را احراز هویت می‌کنند.

---

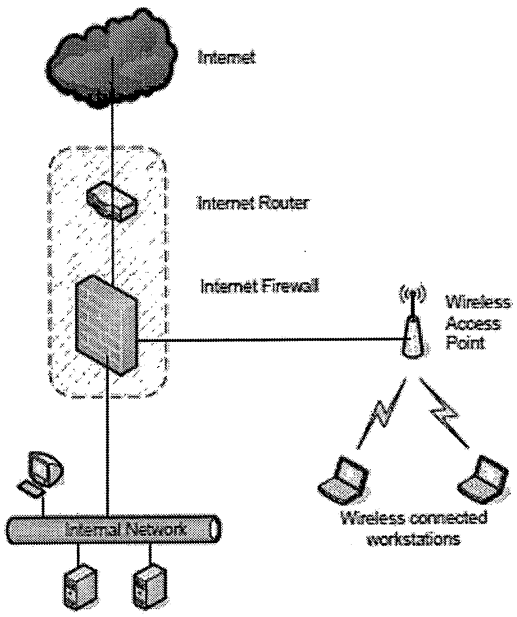
۴۰ Proxy

۴۱ Inner Firewall

۴۲ Control Point

- اطلاعات منتقل شده روی شبکه‌های بی‌سیم باید از طریق راه‌حل رمزگذاری VPN انتها به انتها، رمزگذاری شود.
- نشت و کمبود سیگنال باید از طریق انتخاب مناسب قدرت سیگنال و انتخاب مناسب مکان نقطه‌ی دسترسی بی‌سیم[۴۳] به حداقل برسد.
- احراز هویت بسیار قوی باید برای همه‌ی مشتریان بی‌سیم در حال اتصال به شبکه بکار گرفته شود.
- مواردی که مهمانان نیاز به دسترسی اینترنت از طریق اتصالات بی‌سیم را دارند، این دسترسی باید مطابق قوانین ذکر شده در بخش ۲-۵ انجام گیرد.

نمودار ۲ راه‌کار پیشنهادی جهت پیاده‌سازی ساختار اتصالات بی‌سیم را نشان می‌دهد.

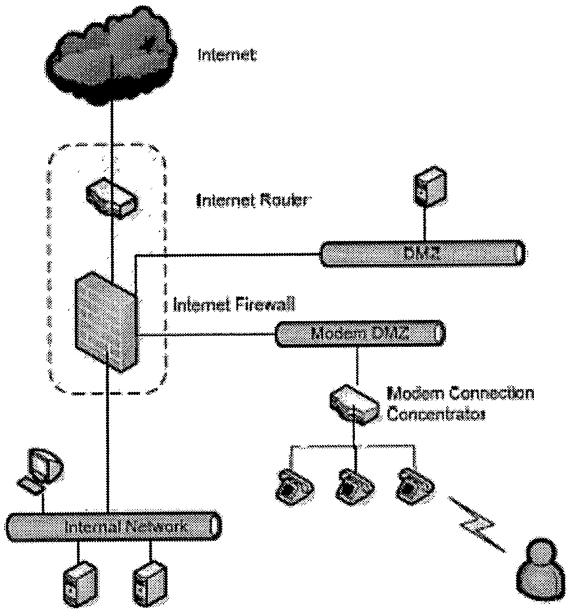


نمودار ۲. نمودار طراحی اتصال بی‌سیم

۵,۲,۲,۲ اتصالات مودم

نمودار ۳ راه‌کار پیشنهادی جهت پیاده‌سازی ساختار اتصالات مودم را نشان می‌دهد.

[۴۳] Wireless Access Point



نمودار ۳. نمودار طراحی اتصال مودم

- اجازه دسترسی به مدیریت تجهیزات متمرکزکننده‌ی اتصال مودم[۴۴] فقط به آدرس‌های IP داخلی مجاز
- تجهیزات متمرکزکننده‌ی اتصال مودم باید در یک VLAN اختصاصی، مجزا شده از شبکه‌ی داخلی به‌وسیله‌ی یک دیواره‌ی آتش، قرار داده شوند.
- قوانین تصفیه باید بکار گرفته شود تا کاربران مودم فقط به سامانه‌هایی که آن‌ها جهت اهداف تجاری نیاز دارند، اجازه‌ی دسترسی داشته باشند.

۳,۲,۲ اجزاء زیرساخت شبکه

زیرساخت شبکه شامل اجزاء گفته شده در ادامه‌ی این بخش می‌باشد و هدف امنیت زیرساخت شبکه یعنی امنیت این ادوات است.

۱,۳,۲,۲ توصیه‌هایی برای همه‌ی اجزاء زیرساخت

۱. تجهیزات باید رویدادنگاری[۴۵] سامانه‌ای، امنیتی و محیطی‌شان را به یک کارگزار از راه‌دور جهت برآورده شدن دو هدف امنیت و تحلیل رویدادنگاری بفرستند.

---

[۴۴] Modem Connection Concentrate

[۴۵] Log

- رویدادنگاری باید حداقل برای دسترسی غیرمجاز پایش شوند.
- برای رویدادنگاری مربوط به دسترسی مجاز/غیرمجاز، تغییرات دستگاه یا تلاش‌ها جهت نفوذ، مدت زمان برخط[۴۶] و برون‌خط[۴۷] بودن رویدادنگاری را تعیین می‌کند. در صورت نبودن این اطلاعات رویدادنگاری باید به صورت پیش‌فرض برای مدت سه ماه برخط و به مدت یک سال برون‌خط نگه داشته شود.
- رویدادنگاری باید روی یک شبکه مدیریتی اختصاصی فرستاده شوند.

۲. پروتکل‌های امن. تجهیزات باید جهت بیشینه کردن اثر راهبری و امنیت، قادر به مدیریت توسط پروتکل‌های دسترسی امن متعدد از طریق روش‌های گوناگون باشند.

- پروتکل‌های ناامن (مانند Talent) اگر از نظر فنی امکان دارد، باید غیرفعال شده و با پروتکل‌های امن (مانند SSH) جایگزین شوند.
- اگر مدیریت وب در دسترس است، نیاز است تا SSL از محرمانه بودن ترافیک حمایت کند و اجازه دهد تا کاربران سایت را احراز هویت کنند.

۳. روند مدیریت تغییرات (CM[۴۸]) باید هر اتفاقی در تجهیزات شبکه را کنترل کند. این فرایند باید صحت و دسترس‌پذیری شبکه را از طریق استقرار مجدد پیکربندی قبلی، زمانیکه یک تغییر سبب کاهش یا از بین رفتن امنیت می‌شود؛ اصلاح کند.

راهبران شبکه باید:

- پشتیبان‌گیری از پیکربندی‌های تجهیزات به یک سامانه‌ی خارجی جهت برآورده شدن دو هدف مدیریت تغییر پیکربندی و امنیت پیکربندی
- پیاده‌سازی کنترل نسخه نرم‌افزار[۴۹] برای میان افزار[۵۰] و/یا سیستم‌عامل
- گرفتن و دنبال کردن اطلاعات آدرس IP : زیرشبکه‌ها، IPهای میزبان بحرانی، نامگذاری قراردادها (DNS[۵۱]) و ... .
- بهره‌گیری از پیکربندی استاندارد (مثلا ادوات باید به‌طور مشابه پیکربندی شوند)
- قادر به دنبال کردن تغییرات ایجاد شده در ادوات باشند (چه کسی و چه زمانی)
- ایجاد و نگهداری به‌روز مستندات توپولوژی شبکه

---

۴۶ Online
۴۷ Offline
۴۸ Change Management
۴۹ Software version control
۵۰ Firmware
۵۱ Domain Name System

- اگر ادوات بحرانی یا خیلی بحرانی هستند، برای فایل‌های پشتیبان پیکربندی دستگاه از امضای دیجیتال یا چکیده‌سازها[۵۲] استفاده شود.

۴. ادوات باید منابع تغذیه متعدد داشته باشند یعنی هرکدام به مدارات تغذیه جداگانه با توان مناسب و در صورت امکان منابع تغذیه اضطراری وصل شوند.

۵. راهبران شبکه باید همه‌ی زمان‌های سامانه را جهت همبستگی حوادث، همزمان کنند.

۶. راهبران شبکه باید همه‌ی کلمه‌های عبور پیش‌فرض دستگاه، شامل کلمه‌ی عبور پیش‌فرض روی درگاه سریال (مثلا برای سوئیچ‌ها[۵۳] و مسیریاب‌ها) را تغییر دهد.

۷. اگر قرار نیست از پروتکل SNMP[۵۴] استفاده شود، راهبران شبکه باید آن را غیرفعال کنند. در صورت استفاده از SNMP، راهبران باید:

- SNMP نسخه‌ی ۳ را به‌جای نسخه‌ی ۱، ۲ یا ۲/۵ بکار ببرند.
- ترافیک ورودی/خروجی SNMP در محیط را تصفیه و ترافیک SNMP داخلی را به ACLs محدود کند.
- جداسازی SNMP به صورت یک شبکه‌ی مدیریت اختصاصی

۸. دسترسی مدیریت باید به انتخاب آدرس‌های IP از طریق استفاده از ACLها محدود شود.

۹. راهبران شبکه باید ادوات را به‌وسیله‌ی غیرفعال ساختن خدمات غیرضروری مقاوم سازند.

۱۰. برای تضمین صحت تجهیزات لازم است تا تجهیزات شبکه تنها از تولید کننده یا فروشندگانی که توسط تولید کننده تجهیزات، مجاز و تائید شده‌اند، خریداری گردد.

۱۱. باید پیش از نصب میان افزار و یا سیستم عامل جدید بر روی تجهیزات شبکه، با مقایسه کد درهمسازی میان افزار تجهیزات شبکه با کد درهمسازی که تولید کننده منتشر نموده، از صحت آن اطمینان ایجاد نمود و باید از نصب و اجرای نسخه‌هایی از میان افزار تجهیزات شبکه که تولید کننده در دسترس قرار نداده، جلوگیری گردد.

۱۲. بر روی شبکه، واسطهای فیزیکی که بر روی تجهیزات شبکه استفاده نمی‌شوند باید خاموش یا غیر فعال گردند و با ایجاد لیست دسترسی (که تنها درگاه‌ها، پروتکل‌ها و آدرس‌های IP را که کاربران شبکه وخدمات به آنها نیاز دارند، مجاز می‌کند و هرچیزی جز موارد ذکر شده در لیست رد می‌شود)،

---

[۵۲] Hash

[۵۳] Switch

[۵۴] Simple Network Management Protocol

دسترسی به تجهیز محدود شود. همچنین خدمات غیر ضروری بر روی تجهیزات شبکه باید خاموش شوند.

۱۳. از افشاء غیرمجاز فایل‌های پیکربندی تجهیزات شبکه باید محافظت گردد، بدین منظور باید مراحلی در نظر گرفته شود که از ظاهر شدن کلمه عبور به صورت آشکار (بدون آنکه رمز شود) جلوگیری می‌نماید.

- استفاده نمودن از رمزنگاری یا درهمسازی با تکرار جهت حفاظت از محرمانگی کلمه عبور در فایل-های پیکربندی لازم و ضروری می‌باشد، لازم به ذکر است کدگذاری به تنهایی کافی نمی‌باشد.
- در صورتیکه فایل پیکربندی تجهیزات شبکه به صورت آشکار منتقل شود و در برگیرنده‌ی کلیدها/کلمه عبورهای رمز نشده باشد، بلافاصله باید کلمه عبورها/کلیدها را تغییر داد.
- از پروتکل‌های امن هنگام انتقال فایل‌های پیکربندی تجهیزات شبکه باید استفاده گردد.

۱۴. باید از تولید رویدادهای ممیزی، در هنگام راه‌اندازی مجدد و ضمن اعمال تغییرات پیکربندی به تجهیزات شبکه اطمینان یافت و گزارش‌های شبکه باید به صورت دوره‌ای بررسی شوند تا فهم عمیقی نسب به رفتار شبکه نرمال حاصل آید.

۱۵. سند کتبی خطمشی امنیتی زیر ساخت شبکه باید ایجاد و نگهداری شود. این سند باید مشخص نماید که چه افرادی مجاز به ورود تجهیزات زیرساخت شبکه هستند و چه کسی مجاز به پیکربندی تجهیزات شبکه می‌باشد.

- همچنین باید طرحی را برای بروزرسانی میان افزار تجهیزات شبکه در فواصل زمانی مشخص تعریف نماید.
- از نام‌های کاربری و کلمه‌عبورهای متداول نباید استفاده شود.
- خط‌مشی زیرساخت شبکه باید الزاماتی بر روی طول کلمه عبور و پیچیدگی آن تعریف نماید.

۱۶. تنها از استانداردهای پروتکل امن در زمان مدیریت نمودن از راه دور تجهیزرات شبکه باید استفاده شود. برای آگاهی بیشتر به پیوست الف از سند پروفایل حفاظتی تجهیزات شبکه مراجعه شود.

۱۷. اتصالات مدیریت از راه دور باید تنها به ماشین‌های کنترل شده‌ای محدود گردد که بر روی یک دامین امنیتی مجزا با حفاظت قوی هستند.

۱۸. از حداقل دو NTP تائید شده برای حفظ یک زمان ثابت بین تجهیزات شبکه باید استفاده شود.

۱۹. در بحث امنیت زیر ساخت شبکه باید از پروتکل‌ها و الگوریتم‌هایی استفاده شود که مورد تائید باشند.

۲۰. در هنگام مدیریت از راه دور تجهیزات شبکه باید از راهنمای استاندارد NIST SP 800-131A برای الگوریتم‌های رمزنگاری و اندازه کلید تبعیت گردد.

۲۱. هنگام استفاده از پروتکل SNMP، باید از SNMP v3 با فعال نمودن رمزنگاری استفاده شود و/یا تمام ترافیک شبکه در یک تونل IPsec کپسوله گردد.
۲۲. تمام VPN های IPsec باید مطابق با استاندارد های IETF و راهنمای NIST SP 800-131A باشند. و در صورت امکان استانداردهای پروتکل امن IETF بکار برده شود.
۲۳. با استناد به استاندارد FIPS 140، باید موتور (یا هسته) رمزنگاری در تجهیزات شبکه مورد ارزیابی قرار گیرد، و الگوریتم‌های انتخاب شده‌ای که با توجه به ارزیابی پروفایل حفاظتی تجهیزات شبکه معتبر گردیده‌اند، پیکربندی گردد.
۲۴. از رویدادنگاری امن [۵۵] به منظور ردیابی اطلاعات امنیتی در سامانه یا زیرساخت شبکه استفاده می‌شود.
۲۵. برای رویدادنگاری امن باید از کارگزار ممیزی از راه دور (همانند Syslog server) استفاده شود. از محرمانگی و صحت و یکپارچگی داده‌های ممیزی باید با برقراری یک اتصال IPsec VPN بین تجهیزات حساس شبکه و کارگزار ممیزی، محافظت گردد.
۲۶. باید اطمینان حاصل گردد که تمام تجهیزات زیرساخت شبکه در زمان اعمال تغییرات پیکربندی، بروزرسانی میان افزار سیستم عامل و همچنین در زمان راه اندازی مجدد تجهیزات، رویداد ممیزی تولید می‌نمایند. همچنین باید اطمینان حاصل گردد که گزارش‌ها براساس یک اسلوب و قاعده بررسی می‌گردند.

۲،۳،۲،۲ دیواره‌های آتش

دیواره‌های آتش باید مطابق با ملزومات زیر پیکربندی گردند:

- بکارگیری قانون رد صریح اگر هیچ قانون دیگری درنظر گرفته نشده باشد.
- اجازه‌ی دسترسی به مدیریت دستگاه فقط به آدرس‌های IP داخلی مجاز داده شود.
- اطمینان از اینکه کلمه‌های عبور سامانه، ملزومات زیر را رعایت می‌کنند: ۱) دارای حداقل ۸ کاراکتر و۲) ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر.
- شامل هیچکدام از قوانین allow all نشود.
- همه‌ی ارتباطات بین مدیریت و دیواره‌ی آتش رمزگذاری شود.
- حصول اطمینان از اینکه ورود عمومی جهت احراز هویت راهبر دیواره‌ی آتش، بکار برده نمی‌شود.
- اطمینان از رمزگذاری همه‌ی کلمه‌های عبور سامانه‌ها هنگام ذخیره در دستگاه

---

[۵۵] Secure Logging

- دیواره‌ی آتش و ادوات امنیت محیط، سرهم شده و به صورت ماهیانه نگه‌داری شود.
- بسته‌های غیر معتبر و جعلی باید رد شوند.
- همه‌ی رویدادنگاری‌های دیواره‌ی آتش باید به یک کارگزار رویدادنگاری، جهت اهداف تحلیل و ذخیری فرستاده شود و حداقل ۳۰ روز نگهداری شود.
- یک دیواره‌ی آتش باید بین هر دو شبکه‌ای با سطوح مختلف اعتماد قرار بگیرد.
- پشتیبان پیکربندی دیواره‌ی آتش نباید روی شبکه‌ای که بوسیله‌ی آن دیواره‌ی آتش محافظت می‌شود، ذخیره شود.
- ماتریسی از کاربردهای شبکه باید با هدف مدیریت هدفمند راهبر شبکه، نگهداری شود. این سبب می‌شود فرایند مدیریت مجموعه‌ی قوانین، به علت ارتباط درست انواع کاربردهای داخلی، بدون خطا انجام شود.
- سیاست‌های دیواره‌ی آتش باید حداقل ۳ ماه یکبار رسیدگی و بازبینی شود.
- آخر همه‌ی قوانین، قانون رد همه‌ی ترافیک باید نوشته شود و همه‌ی ترافیک برمبنای آن توسط دیواره‌ی آتش جلوگیری شود. مگر اینکه یک قانون خاص اجازه‌ی عبور یک نوع از ترافیک را بدهد.
- راهبران شبکه جهت جلوگیری از خدمت باید به حداقل تعداد ممکن از پروتکل‌ها از مبدا به مقصد اجازه‌ی کار بدهند.
- راهبران شبکه باید جهت جلوگیری از نگاشت شبکه و قوانین دیواره‌ی آتش معین، اجازه‌ی ورود پیام‌های منقضی شده‌ی ICMP[۵۶] را ندهند.
- راهبران باید از دسترسی ورود به درگاه‌های ۱۳۵، ۱۳۷، ۱۳۸، ۱۳۹، ۴۴۵ و ۳۳۸۹ جلوگیری کنند مگر برای سامانه‌های خاص. این قانون سبب جلوگیری از ورود از راه دور ویندوز و به اشتراک گذاشتن فایل توسط دیواره‌ی آتش می‌شود.
- راهبران باید آدرس IP عمومی را فقط در جاهای موردنیاز بکار برده و در جاهای دیگر از ترجمه‌ی نشانی شبکه (NAT[۵۷]) و ترجمه‌ی نشانی درگاه (PAT[۵۸]) استفاده کنند.

۳،۳،۲،۲ مسیریاب‌ها و سوئیچ‌ها

مسیریاب‌ها و سوئیچ‌ها باید مطابق با ملزومات زیر پیکربندی گردند:

---

[۵۶] Internet Control Message Port

[۵۷] Network Address Translate

[۵۸] Port Address Translate

- زمانی که یک مسیریاب بر روی یک مرز اعتماد[۵۹] یا سایر مرزهای شبکه‌های منطقی[۶۰] قرار می گیرد، به منظور محدود کردن ارتباطات بین شبکه‌ها، باید فهرست های کنترل دسترسی[۶۱] (ACLs) پیاده‌سازی شوند.
- اطمینان حاصل شود که تمامی کلمه‌های عبور ذخیره شده بر روی دستگاه رمزنگاری شده‌اند.
- اطمینان حاصل شود که برای احرازهویت پیشخوان‌های[۶۲] مدیریت مسیریاب، از ورود عمومی به سامانه-ها استفاده نشود.
- فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه‌ها داده شود.
- تمامی ارتباطات بین پیشخوان مدیریت و مسیریاب‌ها باید رمزنگاری شوند.
- اطمینان حاصل شود که تمامی کلمه‌های عبور سامانه، شرایط زیر را داشته باشند:
  - ✓ حداقل دارای ۸ کاراکتر باشند
  - ✓ ترکیبی از حروف کوچک و بزرگ، اعداد و سایر کاراکترهای خاص باشند.
- اطمینان حاصل شود که حداقل ۲ حساب غیرعمومی[۶۳] که دارای امتیازات راهبری[۶۴] هستند ساخته شده باشد.
- از موارد زیر جلوگیری شود:
  - ✓ خدمات کوچک TCP
  - ✓ خدمات کوچک UDP
  - ✓ امکان اجرای تمامی خدمات وب بر روی دستگاه
- مسیریاب‌ها با توجه به موارد زیر تعمیر و نگهداری شوند:
  - ✓ برای مسیریاب‌هایی که به شبکه‌های خارجی متصل هستند ، هر ۳ ماه یکبار
  - ✓ برای مسیریاب‌هایی که به شبکه‌های خارجی متصل نیستند ، هر ۶ ماه یکبار
- تمامی گزارش‌های مسیریاب به منظور ذخیره‌سازی و تحلیل اتفاقات، باید به یک کارگزار گزارش‌گیری اختصاصی ارسال شوند و این گزارش‌ها باید حداقل ۳۰ روز نگه‌داری شوند.

---

[۵۹] Trust Boundary
[۶۰] Logical Network Boundary
[۶۱] Access Control Lists
[۶۲] Console
[۶۳] Non-Generic Account
[۶۴] Administrative Privileges

- تمامی احرازهویت‌های راهبردی به دستگاه باید از طریق یک کارگزار احرازهویت مرکزی مثل RADIUS انجام پذیرد.
- راهبرها باید تضمین دهند که مسیریاب‌ها و سوئیچ‌ها تحت شرایط زیر قادر به انجام پیکربندی در سطح دستگاه (مثلا منابع تغذیه دوتایی) و در سطح شبکه (مثلا معماری مش) هستند:
  - ✓ غیربحرانی: اختیاری
  - ✓ بحرانی: توصیه شده
  - ✓ به شدت بحرانی: ضروری
- راهبرها باید تضمین کنند که سوئیچ‌ها قادر به فراهم کردن درگاه‌های SPAN به منظور ثبت و تحلیل ترافیک تولید شده هستند (به عنوان مثال، تشخیص و ممانعت از نفوذ در شبکه)
- راهبرها باید موارد زیر را غیرفعال کنند:
  - ✓ خدمات مدیریتی غیرضروری (http، indent و ...)
  - ✓ خدمات کنترلی غیرضروری (bootp، CDP، خدمات کوچک TCP/UDP و ...)
- راهبرها باید گزارش‌گیری را فعال کرده و کارگزاری را برای گزارش‌گیری تخصیص دهند.
- راهبرها باید اطمینان حاصل کنند درگاه‌های سوئیچ به طور پیش‌فرض غیرفعال هستند و به VLANهای مهمان/محدود تنظیم شده‌اند.
- راهبرها باید برای هر درگاه سوئیچ یک آدرس MAC تخصیص دهند.
- راهبرها نباید به سامانه‌های «لبه»[۶۵] تا به دروازه[۶۶]، مسیریاب، یا کارگزاران DHCP/BOOTP تبدیل شوند.
- راهبرها نباید اجازه جعل هویت[۶۷] آدرس‌های IP شبکه‌های خارجی را بدهند.

۴,۳,۲,۲ مسیریاب مرزی با فهرست کنترل دسترسی (ACL)

- مسیریاب‌های مرزی افزونه و همچنین مسیرهای افزونه باید به منظور حذف خرابی‌های تک‌نقطه‌ای در گلوگاه‌ها مورد استفاده قرار گیرند.
- باید از ACLهای پیش‌فرض به منظور حفاظت از آدرس‌های IP و درگاه‌هایی که آسیب‌پذیر شناخته می‌شوند مورد استفاده قرار گیرند.

---

[۶۵] Edge

[۶۶] Gateway

[۶۷] Spoofing

- پروتکل‌هایی که معمولا برای مدیریت سیستم به‌کار می‌روند (مثل SSH) باید در مرزها از آدرس‌های IP خارجی شناخته شده محافظت کنند.
- تغییر مداوم و دوره‌ای رویه‌های مدیریتی باید ACLها را به صورت منظم بازبینی، اضافه و یا حذف کنند.
- هر پروتکل و یا هر نوع ترافیکی که توسط سیاست‌های امنیتی سازمان‌ها ممنوع شده‌اند باید توسط پالایش‌گر بسته‌های مسیریاب مرزی مسدود شوند. این امر، پیاده‌سازی سیاست‌های امنیتی خاص را متمرکز می‌کند، و ترافیک و گزارش‌های دیواره‌های آتش را کاهش می‌دهد.
- ACLهای توصیه شده در جدول موجود در لینک زیر فهرست شده‌اند. این فهرست مبتنی بر راهنمای موسسه ملی استاندارد و فناوری (NIST) برای دیواره‌های آتش و سیاست دیواره آتش می‌باشد.

http://csrc.nist.gov/pubications/nistpubs/800-41/sp800-41.pdf

۵,۳,۲,۲ سوئیچ‌های LAN

سوئیچ‌های LAN باید مطابق با ملزومات زیر پیکربندی گردند:

- اطمینان حاصل شود که تمامی کلمه‌های عبور سامانه، شرایط زیر را داشته باشند:
  - ✓ حداقل دارای ۸ کاراکتر باشند
  - ✓ ترکیبی از حروف کوچک و بزرگ، اعداد و سایر کاراکترهای خاص باشند.
- فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه ها داده شود.
- اطمینان حاصل شود که تمامی رمز عبورهای ذخیره شده بر روی دستگاه رمزنگاری شده‌اند.
- اطمینان حاصل شود که برای احرازهویت پیشخوان‌های مدیریت مسیریاب، از ورود عمومی به سامانه‌ها استفاده نشود.
- اطمینان حاصل شود که حداقل ۲ حساب غیرعمومی[۶۸] که دارای امتیازات راهبردی[۶۹] هستند ساخته شده باشد.
- سوئیچ‌ها باید هر دو سال یک‌بار تعمیر و نگهداری شوند اطمینان حاصل شود که تمامی درگاه‌های بدون استفاده سوئیچ به وضعیت خاموش تنظیم شده باشند.

---

[۶۸] Non-Generic Account

[۶۹] Administrative Privileges

- تمامی گزارش‌های مسیریاب به منظور ذخیره‌سازی و تحلیل اتفاقات، باید به یک کارگزار گزارش‌گیری اختصاصی ارسال شوند و این گزارش‌ها باید حداقل ۳۰ روز نگه‌داری شوند.
- پیکربندی VLAN Trunking را بر روی درگاه‌هایی از سوئیچ که نیازی به این پیکربندی ندارند غیرفعال شود.
- به هنگام استفاده از trunking بر روی درگاه‌های شبکه، پروتکل trunking باید تعیین شود. به سوئیچ‌ها اجازه داده نشود تا با پروتکل‌های trunking تبادل اطلاعات کنند.
- از پل زدن بین دو یا چند VLAN ممانعت شود. اگر نیازی به برقراری ارتباط بین VLANها بود، باید یک سوئیچ لایه ۳ پیاده‌سازی شده و مسیریابی فعال گردد.

۶,۳,۲,۲ شتاب‌دهنده‌ی پهنای‌باند[۷۰]/دستگاه‌های اولویت‌بندی

شتاب‌دهنده‌ی پهنای‌باند/دستگاه‌های اولویت‌بندی باید مطابق با ملزومات زیر پیکربندی گردند:

- اطمینان حاصل شود که تمامی کلمه‌های عبور ذخیره شده بر روی دستگاه رمزنگاری شده‌اند.
- اطمینان حاصل شود که برای احرازهویت پیشخوان‌های مدیریت مسیریاب، از ورود عمومی به سامانه‌ها استفاده نشود.
- فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه ها را داده شود.
- تمامی ارتباطات بین پیشخوان مدیریت و شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی باید رمزنگاری شوند.
- اطمینان حاصل شود که تمامی رمز ورودهای سیستم، شرایط زیر را داشته باشند:
  - حداقل دارای ۸ کاراکتر باشند.
  - ترکیبی از حروف کوچک و بزرگ، اعداد و سایر کازاکترهای خاص باشند.
- اطمینان حاصل شود که حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده باشد.
- شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی با توجه به موارد زیر تعمیر و نگهداری می‌شوند:
  - ✓ برای شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی که به شبکه‌های خارجی متصل هستند ، هر ۳ ماه یکبار

---

[۷۰] Bandwidth Accelerators/Prioritization Devices

- ✓ برای شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی که به شبکه‌های خارجی متصل نیستند ، هر ۶ ماه یکبار

- اطمینان حاصل شود که تمامی خدمات شبکه‌ای لازم برای اهداف تجاری از سایر خدماتی که برای اهداف تجاری نیازی بدان‌ها نیست، اولویت بالاتری دریافت می‌کنند.

۷,۳,۲,۲ دستگاه‌های متمرکز کننده مودم[۷۱]

- اطمینان حاصل کنید که تمامی رمز عبورهای ذخیره شده بر روی دستگاه رمزنگاری شده‌اند
- اطمینان حاصل کنید که برای احرازهویت پیشخوان‌های مدیریت مسیریاب، از ورود عمومی به سیستم-ها استفاده نشود
- فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه ها را بدهید
- تمامی ارتباطات بین پیشخوان مدیریت و شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی باید رمزنگاری شوند
- اطمینان حاصل کنید که تمامی رمز ورودهای سیستم، شرایط زیر را داشته باشند:
  - ✓ حداقل دارای ۸ کاراکتر باشند
  - ✓ ترکیبی از حروف کوچک و بزرگ، اعداد و سایر کاراکترهای خاص باشند
- اطمینان حاصل شود که حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده باشد.
- دستگاه‌های متمرکزکننده‌ی مودم با توجه به موارد زیر تعمیر و نگهداری می‌شوند:
  - ✓ برای مسیریاب‌هایی که به شبکه‌های خارجی متصل هستند ، هر ۳ ماه یکبار
  - ✓ برای مسیریاب‌هایی که به شبکه‌های خارجی متصل نیستند ، هر ۶ ماه یکبار
- اطمینان حاصل شود که تمامی درگاه‌هایی از مودم که استفاده نشده‌اند، از کار انداخته شده باشند[۷۲]
- اطمینان حاصل شود که تمامی کاربرانی که به شبکه CGIAR متصل می‌باشند، قبل از آن‌که به آن‌ها اجازه دسترسی داده شود، به گونه‌ای مطلوب احراز هویت شده باشند.
- اطمینان حاصل شود که تصفیه مناسبی پیاده‌سازی شده باشد به گونه‌ای که کاربران مودم فقط بتوانند به سامانه‌هایی دسترسی پیدا کنند که بدان‌ها برای اهداف تجاری نیاز دارند.

---

[۷۱] Modem Concentrator Devices

[۷۲] Disabled

۸,۳,۲,۲ فیلتر کننده های مبتنی بر محتوی [۷۳]

- فیلتر کننده های مبتنی بر محتوی باید از ترکیبی از «فهرست‌های سیاه» و «فهرست‌های سفید» استفاده کنند.
- فیلتر کننده های مبتنی بر محتوی باید با توجه مشاوره‌های امنیتی فروشنده اصلاح و نگهداری شوند
- امضاهای پالایش‌گرهای محتوا باید به صورت روزانه به‌روز رسانی شوند.
- گزارشی شامل فعالیت‌های پالایشی (به خصوص تلاش‌های صورت گرفته برای دسترسی غیرمجاز به محتواها) باید به صورت روزانه تولید و توسط مدیر IT بازبینی شوند.

۹,۳,۲,۲ آنتی‌ویروس‌ها

- دروازه‌های آنتی‌ویروس به منظور پایش ترافیک وب و ایمیل ورودی و خروجی برای تشخیص فعالیت-های مشکوکی که دلالت بر وجود یک ویروس یا بدافزار دارند پیاده‌سازی شوند.
- اتصالات شبکه‌ای از سوی ایستگاه‌های‌کاری[۷۴] به شبکه‌های داخلی و اینترنت باید مسدود شوند تا از گسترش و فعالیت بدافزارها ممانعت شود.

۱۰,۳,۲,۲ نقاط دسترسی بی‌سیم

- پیشخوان راهبری نباید از طریق شبکه رادیویی بی‌سیم قابل دسترسی باشد.
- نقاط دسترسی بی‌سیم باید در پاسخ به هشدارهای محصول که توسط فروشنده سخت‌افزار منتشر می-شوند تعمیر و نگهداری شوند.
- تمامی کارخواه‌هایی[۷۵] که به نقطه دسترسی بی‌سیم هستند باید از رمزنگاری‌های قوی استفاده کنند (مثلا از WPAv1 و WPAv2 استفاده کنند)
- تمامی شبکه‌های بی‌سیم باید به یک VLAN مجزا ختم شوند. باید از احرازهویت قوی در قالب استاندارد 802.1x استفاده شود.
- راهبران باید از POA یا مسئول آن برای نصب یک AP مجوز بگیرند.

---

[۷۳] Content Filters

[۷۴] Workstations

[۷۵] Clients

- راهبران باید به منظور آگاهی ISO، قبل از نصب و راه‌اندازی نقاط دسترسی بی‌سیم که برای پردازش و ارسال داده‌های طبقه‌بندی شده مورد استفاده قرار خواهد گرفت با POA همکاری کنند.
- راهبران باید سایت را مورد بررسی قرار دهند تا پوشش‌دهی لازم برای منطقه مورد نظر را اندازه‌گیری کرده و فراهم سازند.
- راهبران باید قبل از خرید اطمینان حاصل کنند که دستگاه از ارتقاء میان افزار[۷۶] پشتیبانی می‌کند به گونه‌ای که بسته‌های امنیتی به محض در دسترس بودن نصب شوند.
- راهبران باید به هنگام خرید دستگاه‌ها تایید کنند که آن‌ها از ملزومات محافظت از هر سطحی از اطلاعات و طبقه‌بندی سیستم پشتیبانی می‌کنند.
- راهبرها باید تمامی APهای متصل به شبکه‌های دانشگاهی را ثبت کنند.
- راهبرها باید پشتیبانی[۷۷] از تمامی نرم‌افزارها، راهنمای نصب، و رویه‌های لازم برای پشتیبانی از شبکه-های بی‌سیم را جمع‌آوری و ذخیره کنند.
- راهبرها باید به گونه‌ای مطلوب، تمامی APها را به دور از دسترس نصب کنند تا از حملات مهاجمینی که می‌توانند یک نقطه دسترسی تقلبی ناامن را به جای نقطه دسترسی حفاظت شده جایگزین کنند، ممانعت به عمل آورند.
- راهبر باید ارزیابی از ریسک داشته باشد تا از پیکربندی صحیح دستگاه‌های بی‌سیم و امنیت اطلاعات اطمینان حاصل کند.
- راهبر باید محدوده‌ی نقاط دسترسی را بررسی کند و اطمینان حاصل کند که محدوده پوشش‌دهی فقط دستگاه‌های نیازمند دسترسی را شامل می‌شود.
- راهبر باید مطمئن شود که عملیات راه‌اندازی مجدد نقاط دسترسی فقط به هنگام ضرورت انجام پذیرد، و فقط توسط افراد مجاز ممکن باشد.
- راهبر باید ارتباطات بی‌سیم را از دسترسی مستقیم به سامانه‌هایی که بر روی شبکه سیمی قرار دارند چه به صورت فیزیکی و چه به صورت نرم‌افزاری جدا کند.
- راهبر باید در مواردی که امکان دارد، انتشار امواج رادیویی را در خارج از منطقه مورد نیاز با استفاده از آنتن‌های قابل هدایت کاهش دهد.
- راهبر باید SSID نقاط دسترسی را تغییر دهد.

---

[۷۶] Firmware Upgrades

[۷۷] Backup

پیشنهادات امنیتی برای امن‌سازی زیرساخت شبکه

- راهبر باید همه‌پخشی مشخصه SSID را غیرفعال کند به گونه‌ای که SSID کارخواه باید با SSID نقطه دسترسی منطبق باشد.
- راهبر باید اطمینان حاصل کند که رشته کاراکتری SSID از هیچ نامی که بتواند با نام دانشگاه تداعی شود استفاده نکند.
- راهبر باید اطمینان حاصل کند که تمامی دستگاه‌ها باید دارای رمز عبورهای راهبری قوی باشند.
- راهبر باید تضمین حاصل کند که تمامی پیکربندی‌های پیش‌فرض غیرضروری تغییر کرده باشند.
- راهبر باید تمامی پروتکل‌های غیرضروری را بر روی دستگاه بی‌سیم غیرفعال کند.
- اگر دستگاه بی‌سیم از گزارش‌گیری پشتیبانی می‌کند، باید روشن باشد و گزارش‌ها به طور مرتب بازبینی شوند.
- راهبر باید اطمینان حاصل کند که نقاط دسترسی به هنگامی که از آن‌ها استفاده نمی‌شود خاموش باشند.
- راهبر باید هر نقطه دسترسی غیرمجازی که به شبکه دانشگاه تنسی متصل هستند را غیرفعال و حذف کند.
- راهبر باید مطئن باشد که ترافیک مدیریتی مربوط به دستگاه بی‌سیم بر روی یک زیرشبکه‌ی اختصاصی و جزا باشد.
- راهبر باید به هنگام راهبری از راه دور دستگاه‌های بی‌سیم، از مدهای امن انتقال مثل HTTPS و SSH استفاده کند.

۱۱,۳,۲,۲ دستگاه‌های **VPN**

- به مدیریت دستگاه VPN اجازه داده شود تا فقط به آدرس‌های IP داخلی مجاز دسترسی پیدا کند.
- دستگاه‌های VPN باید در پاسخ به هشدارهای محصول که توسط فروشنده سخت‌افزار یا نرم‌افزار منتشر می‌شوند تعمیر و نگهداری شوند.
- دستگاه‌های VPN باید در یک منطقه حائل (بخشی از IP شبکه) اختصاصی قرار گیرند.
- باید قوانین پالایش به‌کار بسته شوند تا به کاربران VPN اجازه داده شود که صرفا به سامانه‌هایی که برای دسترسی به اهداف تجاری بدان‌ها نیاز دارند متصل شوند.

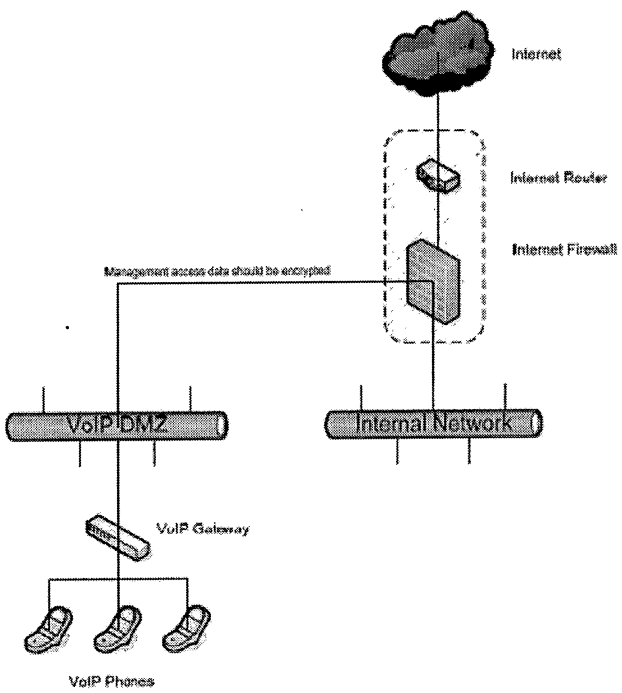
۱۲,۳,۲,۲ کارگزارهای نماینده‌ی وب

- به مدیریت کارساز نماینده اجازه داده شود تا فقط به آدرس‌های IP داخلی مجاز دسترسی پیدا کند.

- هر نماینده باید صرفا طوری پیکربندی شود که فقط اجازه جریان ترافیک در یک جهت را بدهد.
- نماینده‌ها باید در پاسخ به هشدارهای محصول که توسط فروشنده سخت‌افزار یا نرم‌افزار منتشر می‌شوند تعمیر و نگهداری شوند.
- تمامی کاربران نماینده باید وادار شوند تا قبل از دسترسی به اینترنت یا سایر خدمات مجاز احراز هویت شوند.

۱۳،۳،۲،۲ دروازه‌ی VoIP

- به مدیریت دروازه VoIP اجازه داده شود تا فقط به آدرس‌های IP داخلی مجاز دسترسی پیدا کند.
- تمامی ترافیک دسترسی مدیریت باید رمزنگاری شوند.
- اطمینان حاصل شود که تمامی کلمه‌های عبور سامانه، شرایط زیر را داشته باشند:
  - ✓ حداقل دارای ۸ کاراکتر باشند
  - ✓ ترکیبی از حروف کوچک و بزرگ، اعداد و سایر کاراکترهای خاص باشند
- اطمینان حاصل شود که حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده باشد.
- اجازه دسترسی خارجی به ثبات[۷۸] کاربر داخلی که در سامانه VoIP پیکربندی شده است داده نشود.
- دروازه‌های VoIP باید در پاسخ به هشدارهای محصول که توسط فروشنده دروازه‌ها منتشر می‌شوند تعمیر و نگهداری شوند.
- نشست‌های VoIP باید رمزنگاری شوند.



[۷۸] Register

نمودار ۴. نمودار طراحی اتصال VOIP

۱۴,۳,۲,۲ سیستم تشخیص نفوذ / جلوگیری از نفوذ[۷۹] (IDPS)

- مدیریت دسترسی باید فقط به آدرس‌های IP داخلی مجاز محدود شود.
- تمامی ارتباطات بین پیشخوان مدیریت و دستگاه باید رمزنگاری شوند.
- واسط‌های شبکه که برای پایش و جمع‌آوری ترافیک شبکه مورد استفاده قرار می‌گیرند نباید با یک آدرس IP پیکربندی شوند.
- اطمینان حاصل شود که تمامی رمز ورودهای سیستم، شرایط زیر را داشته باشند:
  - ✓ حداقل دارای ۸ کاراکتر باشند
  - ✓ ترکیبی از حروف کوچک و بزرگ، اعداد و سایر کاراکترهای خاص باشند
- اطمینان حاصل شود که حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبری هستند ساخته شده باشد.
- دستگاه‌ها باید در پاسخ به سیستم‌عامل و هشدارهای محصول که توسط فروشنده‌های مربوطه منتشر می‌شوند تعمیر و نگهداری شوند.
- به روز رسانی دوره‌ای امضاء باید از سوی فروشنده قابل دسترس باشد. بین انتشار امضاءهای جدید توسط فروشنده و دریافت آن‌ها توسط IDPS نباید بیش از یک هفته فاصله باشد.
- یک رویه‌ی مدیریتی انجام تغییرات که به طور خاص برای IDPS طراحی شده است باید توسعه یابد و با توجه به به‌روزرسانی‌های امضاءهای جدید اعمال گردند.

---

[۷۹] Network Intrusion Detection/Prevention Systems

- ترافیک پایش شده نباید از پهنای باند IDPS و درگاه سوئیچ بیشتر شود. زمانی که پهنای باند بر روی یک اتصال شبکه‌ای موجود و یا اتصال شبکه‌ی جدید افزایش می‌یابد، راهبران شبکه باید ابتدا ظرفیت را محاسبه کنند تا مطمئن شوند که IDPS جدید نیازمندی‌های پهنای باند را برآورده می‌کند یا خیر.
- IDPS باید قادر باشد تا بسته‌های جدا ازهم مربوط به سیستم‌عامل‌های مختلف را به هم متصل کند.
- IDPS باید قادر به گزارش‌گیری بر روی یک سامانه پایگاه داده باشد.
- IDPS باید قابلیت تنظیم قوانین و سفارشی‌سازی آن‌ها را داشته باشد.
- یک رویه‌ی مدیریتی انجام تغییرات باید توسعه یابد و با توجه به تنظیمات صورت گرفته برای قوانین اعمال گردد.
- سیستم‌های IDPS باید دارای چندین کارت واسطه‌ی شبکه باشند که یکی از آن‌ها بتواند در برابر سایر سامانه‌ها نامرعی[۸۰] و یا فقط قابل خواندن باشد.
- جایابی IDPS بر روی یک شبکه خاص باید بر مبنای طبقه‌بندی اطلاعات بر روی آن شبکه صورت گیرد.
- راهبرها باید حسگرهای IDPS را بر روی هر نوع شبکه‌ای که احتمال درز اطلاعات در آن می‌رود قرار دهند. IDPS می‌تواند به گونه‌ای تنظیم شود تا درز اطلاعات به خارج از شبکه را پایش و گزارش‌دهی کند.
- راهبرها باید مراقب ارسال چندین VLAN به IDPS باشند. اگر سخت‌افزار سوئیچ قادر به ارسال چندین VLAN به یک درگاه SPAN نباشد، سیستم عامل حسگر IDPS باید به منظور تشخیص برچسب‌های VLAN ID و ارسال هر VLAN به واسط مجازی خودش بر روی سامانه از 802.1qپشتیبانی کند.
- راهبرها باید مراقب درگاه‌های SPAN به عنوان روشی برای هدایت ترافیک به IDPS باشند (به خصوص اگر سوئیچ چندین درگاه را به یک درگاه SPAN هدایت می‌کند). مجموع پهنای باند تمامی درگاه‌ها نباید از پهنای باند درگاه SPAN فراتر رود. همچنین راهبرها باید تشخیص دهند که آیا بسته‌های بیش‌از حد بزرگ/کم‌تر از حد کوچک و بسته‌هایی با خطاهای CRC مهم هستند یا خیر چراکه سوئیچ ممکن است آن‌ها را بر روی درگاه SPAN تکثیر نکند. تاخیر نیز یکی از نگرانی‌ها در مورد درگاه SPAN است، اما یک network tap می‌تواند بر این محدودیت‌ها فائق آید.
- راهبرها باید سامانه‌ها و انواع ترافیکی که هر IDPS پایش می‌کند را بشناسند.

---

[۸۰] Invisible

- راهبرها باید قوانینی که برای آن‌ها سیستم/کاربرد مرتبطی وجود ندارد را غیرفعال کنند. این امر پهنای باند با ارزش IDPS را از هدر رفتن حفظ می‌کند.
- در مورد سامانه‌های تشخیص متن‌باز مثل Snort، به هنگام اجرای IDPS بر روی سیستم عاملی که بسته‌ها را مجددا بازبینی می‌کند باید احتیاط‌های لازم صورت گیرد.
- راهبرها نباید از هاب برای دسترسی IDPS به ترافیک استفاده کنند. هاب‌ها می‌توانند باعث تاخیر شوند، دارای منابع تغذیه مستقل باشند و نمی‌توانند به گونه‌ای پیکربندی شوند که صرفا دارای درگاه فقط خواندنی باشند.
- راهبرها باید مراقب استفاده از نماینده‌های SSL برای پایش ترافیک SSL باشند به خصوص اگر التزامات صنایع حکم کنند که چنین ترافیک‌هایی باید بررسی شوند.
- حسگرهای IDPS باید دارای واسطی بر روی یک شبکه مدیریتی که از ترافیکی تولیدی مجزا است باشند. واسط استماع[۸۱] بر روی شبکه باید فقط خواندنی باشد تا از بروز حمله بر روی IDPS ممانعت به عمل آورد.

۳. چک لیست

در این بخش به ارائه چک لیست امن سازی زیرساخت شبکه پرداخته می‌شود.

بند	توصیه امنیتی	√

[۸۱] Listening

بند	توصیه امنیتی	√
امن سازی کلان شبکه		
	صحت تجهیزات	
۱	تجهیزات شبکه از تولید کننده یا از فروشندگانی که توسط تولید کننده تجهیزات مجاز و تائید شده‌اند، خریداری شده است.	
۲	تجهیزات شبکه، با مقایسه کد درهمسازی میان افزار تجهیزات شبکه با کد درهمسازی که تولید کننده منتشر نموده، از صحت آن اطمینان ایجاد نموده است.	
۳	از نصب و اجرای نسخه‌هایی از میان افزار تجهیزات شبکه که تولید کننده در دسترس قرار نداده، جلوگیری گردیده است.	
۴	واسط‌های فیزیکی که بر روی تجهیزات شبکه استفاده نمی‌شوند خاموش یا غیر فعال شده است.	
۵	با ایجاد لیست دسترسی که تنها دسترسی پورت‌ها، پروتکل‌ها و آدرس‌های IP که کاربران شبکه و سرویس‌ها به آنها نیاز دارند، مجاز می‌کند، دسترسی به تجهیزات محدود شده است.	
۶	سرویس‌های غیر ضروری بر روی تجهیزات شبکه خاموش شده است.	
۷	از افشاء غیرمجاز فایل‌های پیکربندی تجهیزات شبکه محافظت گردیده است.	
۸	از رمزنگاری یا درهمسازی با تکرار جهت حفاظت از محرمانگی کلمه عبور در فایل‌های پیکربندی استفاده شده است.	
۹	از پروتکل‌های امن هنگام انتقال فایل‌های پیکربندی تجهیزات شبکه استفاده گردیده است.	
۱۰	از تولید رویدادهای ممیزی در هنگام راه‌اندازی مجدد و ضمن اعمال تغییرات پیکربندی به تجهیزات شبکه، اطمینان حاصل شده است.	

بند	توصیه امنیتی	√
۱۱	گزارش‌های شبکه به صورت دوره‌ای بررسی شده است.	
	مدیریت امن	
۱۲	سند کتبی خطمشی امنیتی زیر ساخت شبکه ایجاد و نگهداری شده است.	
۱۳	طرحی برای بروزرسانی میان افزار تجهیزات شبکه در فواصل زمانی مشخص تعریف شده است.	
۱۴	از نام‌های کاربری و کلمه‌عبورهای متداول استفاده نشده است.	
۱۵	تنها از استانداردهای پروتکل امن در زمان مدیریت نمودن از راه دور تجهیزات شبکه استفاده شده است.	
۱۶	اتصالات مدیریت از راه دور تنها به ماشین‌های کنترل شده‌ای که بر روی یک دامین امنیتی مجزا با حفاظت قوی هستند، محدود گشته است.	
۱۷	از حداقل دو NTP تائید شده برای حفظ یک زمان ثابت بین تجهیزات شبکه استفاده شده است.	
	استاندارد پروتکل امن + رمزنگاری قوی	
۱۸	در هنگام مدیریت از راه دور تجهیزات شبکه از راهنمای استاندارد NIST SP 800-131A برای الگوریتم‌های رمزنگاری و اندازه کلید تبعیت شده است.	
۱۹	در بحث امنیت زیر ساخت شبکه از پروتکل‌ها و الگوریتم‌هایی که مورد تائید می‌باشد، استفاده شده است.	
۲۰	هنگام استفاده از پروتکل SNMP، از SNMP v3 با فعال نمودن رمزنگاری استفاده شده است.	

بند	توصیه امنیتی	√
۲۱	تمام VPN های IPsec مطابق با استاندارد های IETF و راهنمای NIST SP 800-131A می‌باشند.	
۲۲	در صورت امکان استانداردهای پروتکل امن IETF بکار برده شده است.	
۲۳	با استناد به استاندارد FIPS 140، موتور (یا هسته) رمزنگاری در تجهیزات شبکه مورد ارزیابی قرار گرفته است.	
۲۴	الگوریتم‌های انتخاب شده‌ای که با توجه به ارزیابی پروفایل حفاظتی تجهیزات شبکه معتبر گردیده‌اند، پیکربندی شده است.	
رویدادنگاری امن		
۲۵	از رویدادنگاری به منظور ردیابی اطلاعات امنیتی در سامانه یا زیرساخت شبکه استفاده شده است.	
۲۶	برای رخدادنگاری امن از سرور ممیزی از راه دور (همانند Syslog server) استفاده شده است.	
۲۷	از محرمانگی و صحت و یکپارچگی داده‌های ممیزی با برقراری یک اتصال IPsec VPN بین تجهیزات حساس شبکه و سرور ممیزی محافظت گردیده است.	
۲۸	اطمینان حاصل شده است که تمام تجهیزات زیرساخت شبکه در زمان اعمال تغییرات پیکربندی، بروزرسانی میان افزار سیستم عامل و همچنین در زمان راه اندازی مجدد تجهیزات، رویداد ممیزی تولید می‌نمایند.	
۲۹	اطمینان حاصل شده است که گزارش‌ها براساس یک اسلوب و قاعده بررسی می‌گردند.	
امن‌سازی اجرایی زیرساخت شبکه		

بند	توصیه امنیتی	√
۳۰	ادوات شبکه به صورت امن پیکربندی و با یک روش امن قابل دسترسی هستند.	
۳۱	پروتکل‌های امن برای ارتباطات شبکه بکار برده شده است.	
۳۲	شبکه‌های داخلی و خارجی به طور مناسبی از طریق استفاده از مناطق حائل (DMZ[۸۲]) و ادوات کنترلی (مثل دیواره‌های آتش[۸۳] به صورت امن پیکربندی شده یا جداول کنترل دسترسی مسیریاب)، از یکدیگر جداسازی شده‌اند.	
۳۳	دسترسی از راه دور به شبکه‌های داخلی به صورت امن مدیریت شده است.	
۳۴	شبکه‌های داخلی جهت جلوگیری یا تشخیص مبادرت به برقراری اتصال غیرمجاز و جریان یافتن ترافیک مشکوک، پیکربندی شده است.	
	امن سازی ساختار شبکه‌ی داخلی	
	امنیت خدمات شبکه	
۳۵	اتصال به/ از شبکه‌های خارجی شامل استفاده از خدمات شبکه‌ی امن می‌باشد.	
۳۶	انتشار داده روی اتصالات جهت جلوگیری از محدود شدن به وسیله‌ی اشخاص ثالث، رمزگذاری شده است.	
	ذخیره‌ی اطلاعات مهم روی سامانه‌های متصل به شبکه	
۳۷	اطلاعاتی مانند اطلاعات مالی روی سامانه‌هایی که یا به شبکه‌های دشمن متصل هستند یا به طور مستقیم از آن‌ها قابل دسترس هستند (مثل اینترنت) ذخیره نشده است.	
۳۸	پایگاه داده و کارگزارهای دیگر که چنین اطلاعاتی را ذخیره می‌کنند به طور مستقیم قابل	

[۸۲] Demilitarized Zone

[۸۳] Firewalls

بند	توصیه امنیتی	√
	دسترس از اینترنت نمی‌باشند.	
کنترل اتصال به شبکه		
۳۹	قابلیت اتصال کاربران به شبکه‌ها از طریق روش‌هایی مانند محدود کردن دسترسی شبکه به کاربران خاص در طول زمان‌های معین از روز یا هفته، تا جای ممکن محدود شده است.	
۴۰	از VLANها جهت تسهیل در جداسازی ادوات و میزبان‌های[۸۴] شبکه (خصوصا پایگاه‌های داده و کارگزارها) استفاده شده است.	
۴۱	اتصال پایگاه‌های داده و کارگزارها به اینترنت از طریق استفاده از یک پیشکار[۸۵] صورت می‌گیرد.	
۴۲	پایگاه‌های داده به کارگزارهای مناسب (مانند کارگزارهای فایل، پرینت، رایانامه[۸۶] و کاربرد) موردنیاز جهت قابلیت‌های مناسب متصل می‌شوند.	
۴۳	پایگاه‌های داده داخل یک بخش شبکه با استفاده از درگاه‌های شبکه‌ی مناسب به پیشکار به کار رفته در آن بخش وصل می‌شوند.	
۴۴	پایگاه‌های داده متصل شده به بخش‌های شبکه که به احرازهویت نیاز دارند به منظور احرازهویت کاربر به سامانه‌های خدمات احرازهویت مهمان متصل می‌شوند.	
۴۵	جهت کنترل دسترسی پایگاه‌های داده به کارگزارها، تصفیه سیاست IPsec بکار برده شده‌است.	
خدمات راهبری		

[۸۴] Hosts
[۸۵] Proxy Server
[۸۶] Email

بند	توصیه امنیتی	√
۴۶	دسترسی خدمات راهبری به سامانه‌ها و ادوات، به آدرس‌های IP داخلی مجاز، محدود شده است.	
	محیط‌های توسعه و تست حامی شبکه‌ها	
۴۷	محیط‌های توسعه و تست به منظور جلوگیری از دست رفتن اطلاعات و خطای دسترسی، به شبکه‌های منطقی جداگانه تقسیم شده است.	
۴۸	دسترسی از سامانه‌ها و محیط‌های تست و توسعه به سامانه‌ها یا محیط‌های محصولات تا حداقل میزان لازم محدود شده است.	
۴۹	داده‌های تولیدی از محیط‌های تست و توسعه نمی‌گذرد مگر اینکه کاملا نیاز باشد.	
۵۰	دسترسی به شبکه‌های تست و توسعه به کاربران مجاز محدود می‌شود.	
۵۱	دسترسی محیط‌های در حال تست به اجزاء محیط‌های توسعه به حداقل دسترسی موردنیاز جهت تکمیل رضایت‌بخش فرایند تست محدود شده است.	
	دسترسی مهمان	
۵۲	امکان دسترسی مهمان به تنظیمات شبکه و نهایتا دسترسی به شبکه‌ی داخلی فراهم نمی-شود.	
۵۳	Captive Portal در محل شبکه‌های مهمان گذارده شده است تا مهمانان مجبور به پذیرش شرایط گذاشته شده جهت استفاده‌ی قابل قبول بشوند.	
	دسترسی به کاربردهای داخلی	
۵۴	زمانیکه لازم است کاربرد داخل یک مرکز در دسترس مراکز دیگر قرار بگیرد، این دسترسی از طریق استفاده از شبکه اختصاصی مجازی (VPN) و فقط بر اساس نیاز صورت می‌گیرد.	

بند	توصیه امنیتی	√
دستورالعمل اتصال خارجی		
دسترسی شخص ثالث به شبکه‌های داخلی		
۵۵	اگر نیاز مشروع جهت دسترسی به شبکه‌ی داخلی از طریق اینترنت وجود داشته باشد، دسترسی تنها برای دوره‌ی زمانی محدودی که شخص ثالث بتواند کار تائید شده‌اش را به اتمام برساند، داده می‌شود.	
احراز هویت کاربر برای اتصالات خارجی		
۵۶	دسترسی به داده، خدمات و کاربردهای خارج از دسترس میزبان از طریق اتصالات خارجی، باید فقط به کاربری که به عنوان کاربر مجاز شناسایی و احرازهویت شده باشد، اجازه داده شود.	
۵۷	نباید امکان گذشتن از کنار مرحله‌ی احراز هویت وجود داشته باشد. یک استثناء برای این موضوع دسترسی عموم مردم به کاربردهای در نظر گرفته شده برای استفاده ناشناس می‌باشد.	
۵۸	قدرت سازوکار احراز هویت کاربر بکار برده شده به حساسیت اطلاعات بکار گرفته شده توسط شبکه بستگی دارد.	
۵۹	سازوکار احراز هویت مناسب شامل موارد زیر می‌باشد اما به آن محدود نمی‌شود: • Hardware tokens • تکنیک‌های رمزنگاشتی[۸۷] • پروتکل‌های چالشی-پاسخی[۸۸]	

[۸۷] Cryptographic

[۸۸] Challenge-response

بند	توصیه امنیتی	√
۶۰	هر کاربر جهت اتصال به شبکه‌ی اینترنت باید از طریق VPN و با بکار بستن یک یا چند تکنیک آن که در زیر آمده است متصل شود: • پروتکل L2TP[۸۹] • IPsec • لایه‌ی دریچه‌ی امن (SSL[۹۰]) با استفاده از حداقل رمزگذاری[۹۱] ۱۲۸ بیتی	
	تفکیک اتصالات اینترنت	
۶۱	همه‌ی ترافیک‌های ورودی و خروجی از طریق دیواره‌ی آتش لایه‌ی انتقال یا ادوات معادل دیگر گذشته و به وسیله‌ی آن تصفیه می‌شوند. این دستگاه بعدا به عنوان دیواره‌ی آتش اینترنت یاد می‌شود	
۶۲	دیواره‌ی آتش اینترنت فقط اجازه‌ی دسترسی مجموعه‌ی کمی از انواع سرویس‌های موردنیاز جهت اهداف تجاری را، به و از سیستم‌های شبکه‌ی داخلی می‌دهد.	
۶۳	شبکه‌های تولید، توسعه و تست/پذیرش به صورت فیزیکی جدا شده‌اند.	
۶۴	دیواره‌ی آتش اینترنت و دیواره‌ی آتش مسیریاب ممکن است در برخی سناریوها با هم ترکیب شده و به عنوان یک دستگاه در شکل نشان داده شوند. این بسته به نوع خدمت اینترنت و تکنولوژی ارتباطات بکار گرفته شده جهت خاتمه دادن به آن سرویس از یک کشور به کشور دیگر فرق می‌کند.	
۶۵	هیچ ترافیکی قادر به برقراری ارتباط بین سامانه‌های مواجه با اینترنت و سامانه‌های عدم مواجه با اینترنت بدون گذاشتن و تصفیه شدن بوسیله‌ی دیواره‌ی آتش لایه‌ی کاربرد یا	

[۸۹] Layer 2 Tunneling Protocol

[۹۰] Secure Socket Layer

[۹۱] Encryption

بند	توصیه امنیتی	√
	ادوات معادل (مانند نماینده[۹۲]) نیست. این ادوات دیواره‌ی آتش داخلی[۹۳] نامیده می‌شوند.	
۶۶	هنگام پیاده‌سازی سامانه‌های مواجه با اینترنت، همه‌ی آن‌ها در یک منطقه‌ی حائل اینترنت که بوسیله‌ی دیواره‌ی آتش اینترنت تولید شده، قرار داده می‌شوند.	
۶۷	دیواره‌ی آتش داخلی فقط اجازه‌ی دسترسی مجموعه‌ی کمی از انواع خدمات موردنیاز جهت اهداف تجاری را، به و از سامانه‌های موجود در منطقه‌ی حائل اینترنت می‌دهد.	
۶۸	همه‌ی سامانه‌های منطقه‌ی حائل اینترنت نرم‌افزار آنتی ویروس را به‌صورت نصب شده دارا می‌باشند.	
	اتصالات بی‌سیم	
۶۹	اتصالات بی‌سیم از شبکه‌های داخلی سیمی از طریق حداقل یک نقطه‌ی کنترلی[۹۴] جدا شده‌اند.	
۷۰	شبکه‌های بی‌سیم باید با استفاده از دیواره‌ی آتش لایه‌ی انتقال به‌طور فیزیکی از شبکه‌های دیگر جدا شود.	
۷۱	گره‌های گیرنده و فرستنده یک شبکه‌ی بی‌سیم به صورت دو به دو همدیگر را احراز هویت می‌کنند	
۷۲	نشت و کمبود سیگنال از طریق انتخاب مناسب قدرت سیگنال و انتخاب مناسب مکان نقطه‌ی دسترسی بی‌سیم[۹۵] به حداقل رسیده است.	
۷۳	احراز هویت بسیار قوی برای همه‌ی مشتریان بی‌سیم در حال اتصال به شبکه بکار گرفته	

[۹۲] Proxy
[۹۳] Inner Firewall
[۹۴] Control Point
[۹۵] Wireless Access Point

بند	توصیه امنیتی	√
	شده است.	
اتصالات مودم		
۷۴	اجازه دسترسی به مدیریت تجهیزات متمرکزکننده‌ی اتصال مودم[۹۶] فقط به آدرس‌های IP داخلی مجاز داده می‌شود.	
۷۵	تجهیزات متمرکزکننده‌ی اتصال مودم در یک VLAN اختصاصی، مجزا شده از شبکه‌ی داخلی به‌وسیله‌ی یک دیواره‌ی آتش، قرار داده شده است.	
۷۶	قوانین تصفیه بکار گرفته می‌شود تا کاربران مودم فقط به سامانه‌هایی که آن‌ها جهت اهداف تجاری نیاز دارند، اجازه‌ی دسترسی داشته باشند.	
اجزاء زیرساخت شبکه		
توصیه‌هایی برای همه‌ی اجزاء زیرساخت		
۷۷	ادوات رویدادنگاری[۹۷] سامانه‌ای، امنیتی و محیطی‌شان را به یک کارگزار از راه‌دور جهت برآورده شدن دو هدف امنیت و تحلیل رویدادنگاری می‌فرستند.	
۷۸	رویدادنگاری برای دسترسی غیرمجاز پایش می‌شوند.	
۷۹	برای رویدادنگاری مربوط به دسترسی مجاز/غیرمجاز، تغییرات دستگاه یا تلاش‌ها جهت نفوذ، مدت زمان برخط[۹۸] و برون‌خط[۹۹] بودن رویدادنگاری را تعیین می‌کند.	
۸۰	رویدادنگاری روی یک شبکه مدیریتی اختصاصی فرستاده می‌شوند.	

[۹۶] Modem Connection Concentrate
[۹۷] Log
[۹۸] Online
[۹۹] Offline

بند	توصیه امنیتی	√
۸۱	ادوات جهت بیشینه کردن اثر راهبری و امنیت، قادر به مدیریت توسط پروتکل‌های دسترسی امن متعدد از طریق روش‌های گوناگون می‌باشند.	
۸۲	پروتکل‌های ناامن (مانند Talent) اگر از نظر فنی امکان داشته باشد، غیرفعال و با پروتکل-های امن (مانند SSH) جایگزین می‌شوند.	
۸۳	روند مدیریت تغییرات (CM[۱۰۰]) صحت و دسترس‌پذیری شبکه را از طریق استقرار مجدد پیکربندی قبلی، زمانیکه یک تغییر سبب کاهش یا از بین رفتن امنیت می‌شود؛ اصلاح می-کند.	
۸۴	از پیکربندی‌های ادوات به یک سامانه‌ی خارجی جهت برآورده شدن دو هدف مدیریت تغییر پیکربندی و امنیت پیکربندی توسط راهبران پشتیبان‌گیری می‌شود.	
۸۵	کنترل نرم‌افزار برای میان افزار[۱۰۱] و/یا سیستم‌عامل پیاده‌سازی می‌شود.	
۸۶	از پیکربندی استاندارد بهره‌گیری می‌شود.	
۸۷	تغییرات ایجاد شده در ادوات باشند را دنبال می‌شود.	
۸۸	مستندات توپولوژی شبکه به‌روز نگهداری می‌شود.	
۸۹	اگر ادوات بحرانی یا خیلی بحرانی هستند، برای فایل‌های پشتیبان پیکربندی دستگاه از امضای دیجیتال یا چکیده‌سازها[۱۰۲] استفاده می‌شود.	
۹۰	ادوات منابع تغذیه متعدد دارند یعنی هرکدام به مدارات تغذیه جداگانه با توان مناسب و در صورت امکان منابع تغذیه اضطراری وصل می‌شوند.	

[۱۰۰] Change Management

[۱۰۱] Firmware

[۱۰۲] Hash

بند	توصیه امنیتی	√
۹۱	همه‌ی زمان‌های سامانه جهت همبستگی حوادث، همزمان می‌شوند.	
۹۲	همه‌ی کلمه‌های عبور پیش‌فرض دستگاه، شامل کلمه‌ی عبور پیش‌فرض روی درگاه سریال تغییر داده می‌شوند.	
۹۳	در صورت عدم استفاده از پروتکل SNMP[۱۰۳] آن غیرفعال می‌شود.	
۹۴	در صورت استفاده از پروتکل SNMP نسخه‌ی ۳ به‌جای نسخه‌ی ۱، ۲ یا ۲/۵ بکار برده می‌شود، ترافیک ورودی/خروجی SNMP در محیط تصفیه و ترافیک SNMP داخلی به ACLs محدود می‌شود و SNMP به صورت یک شبکه‌ی مدیریت اختصاصی جداسازی می‌شود.	
۹۵	دسترسی مدیریت به انتخاب آدرس‌های IP از طریق استفاده از ACLها محدود می‌شود.	
۹۶	ادوات به‌وسیله‌ی غیرفعال ساختن خدمات غیرضروری مقاوم می‌شوند.	
۹۷	برای تضمین صحت تجهیزات تجهیزات شبکه تنها از تولید کننده یا فروشندگانی که توسط تولید کننده تجهیزات، مجاز و تائید شده‌اند، خریداری می‌گردد.	
۹۸	پیش از نصب میان افزار و یا سیستم عامل جدید بر روی تجهیزات شبکه، با مقایسه کد درهمسازی میان افزار تجهیزات شبکه با کد درهمسازی که تولید کننده منتشر نموده، از صحت آن اطمینان ایجاد می‌شود.	
۹۹	بر روی شبکه، واسط‌های فیزیکی که بر روی تجهیزات شبکه استفاده نمی‌شوند خاموش یا غیر فعال می‌گردند و با ایجاد لیست دسترسی، دسترسی به تجهیز محدود می‌شود.	
۱۰۰	از رمزنگاری یا درهمسازی با تکرار جهت حفاظت از محرمانگی کلمه عبور در فایل‌های پیکربندی استفاده می‌شود.	

[۱۰۳] Simple Network Management Protocol

پیشنهادات امنیتی برای امن‌سازی زیرساخت شبکه

بند	توصیه امنیتی	√
۱۰۱	اگر فایل پیکربندی تجهیزات شبکه به صورت آشکار منتقل شود و در برگیرنده‌ی کلیدها/کلمه عبورهای رمز نشده باشد، بلافاصله کلمه عبورها/کلیدها تغییر داده می‌شود.	
۱۰۲	از پروتکل‌های امن هنگام انتقال فایل‌های پیکربندی تجهیزات شبکه استفاده می‌گردد.	
۱۰۳	از تولید رویدادهای ممیزی، در هنگام راه‌اندازی مجدد و ضمن اعمال تغییرات پیکربندی به تجهیزات شبکه اطمینان یافته می‌شود.	
۱۰۴	سند کتبی خطمشی امنیتی زیر ساخت شبکه ایجاد و نگهداری می‌شود و مشخص می‌نماید که چه افرادی مجاز به ورود تجهیزات زیرساخت شبکه هستند و چه کسی مجاز به پیکربندی تجهیزات شبکه می‌باشد.	
۱۰۵	تنها از استانداردهای پروتکل امن در زمان مدیریت نمودن از راه دور تجهیزرات شبکه استفاده می‌شود.	
۱۰۶	اتصالات مدیریت از راه دور تنها به ماشین‌های کنترل شده‌ای محدود می‌گردد که بر روی یک دامین امنیتی مجزا با حفاظت قوی هستند.	
۱۰۷	از حداقل دو NTP تائید شده برای حفظ یک زمان ثابت بین تجهیزات شبکه استفاده می-شود.	
۱۰۸	در بحث امنیت زیر ساخت شبکه از پروتکل‌ها و الگوریتم‌هایی استفاده می‌شود که مورد تائیدند.	
۱۰۹	در هنگام مدیریت از راه دور تجهیزات شبکه از راهنمای استاندارد NIST SP 800-131A برای الگوریتم‌های رمزنگاری و اندازه کلید تبعیت می‌گردد.	
۱۱۰	هنگام استفاده از پروتکل SNMP،از SNMP v3 با فعال نمودن رمزنگاری استفاده می‌شود و/یا تمام ترافیک شبکه در یک تونل IPsec کپسوله می‌گردد.	

بند	توصیه امنیتی	√
۱۱۱	تمام VPN های IPsec مطابق با استانداردهای IETF و راهنمای NIST SP 800-131A هستند.	
۱۱۲	با استناد به استاندارد FIPS 140، موتور رمزنگاری در تجهیزات شبکه مورد ارزیابی قرار می‌گیرد، و الگوریتم‌های انتخاب شده‌ای که با توجه به ارزیابی پروفایل حفاظتی تجهیزات شبکه معتبر گردیده‌اند، پیکربندی می‌گردد.	
۱۱۳	از رویدادنگاری امن [۱۰۴] به منظور ردیابی اطلاعات امنیتی در سامانه یا زیرساخت شبکه استفاده می‌شود.	
۱۱۴	برای رویدادنگاری امن از کارگزار ممیزی از راه دور استفاده می‌شود.	
۱۱۵	از محرمانگی و صحت و یکپارچگی داده‌های ممیزی با برقراری یک اتصال IPsec VPN بین تجهیزات حساس شبکه و کارگزار ممیزی، محافظت می‌گردد.	
۱۱۶	تمام تجهیزات زیرساخت شبکه در زمان اعمال تغییرات پیکربندی، بروزرسانی میان فزار سیستم عامل و همچنین در زمان راه اندازی مجدد تجهیزات، رویداد ممیزی تولید می‌نمایند.	
	دیواره‌های آتش	
۱۱۷	قانون رد صریح اگر هیچ قانون دیگری درنظر گرفته نشده باشد، استفاده می‌شود.	
۱۱۸	اجازه‌ی دسترسی به مدیریت دستگاه فقط به آدرس‌های IP داخلی مجاز داده می‌شود.	
۱۱۹	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	

[۱۰۴] Secure Logging

بند	توصیه امنیتی	√
۱۲۰	همه‌ی ارتباطات بین مدیریت و دیواره‌ی آتش رمزگذاری می‌شود.	
۱۲۱	ورود عمومی جهت احراز هویت راهبر دیواره‌ی آتش، بکار برده نمی‌شود.	
۱۲۲	همه‌ی کلمه‌های عبور سامانه‌ها هنگام ذخیره در دستگاه رمزگذاری می‌شود.	
۱۲۳	دیواره‌ی آتش و ادوات امنیت محیط، سرهم شده و به صورت ماهیانه نگه‌داری می‌شوند.	
۱۲۴	بسته‌های غیر معتبر و جعلی رد می‌شوند.	
۱۲۵	همه‌ی رویدادنگاری‌های دیواره‌ی آتش به یک کارگزار رویدادنگاری، جهت اهداف تحلیل و ذخیری فرستاده می‌شود و حداقل ۳۰ روز نگهداری می‌شود.	
۱۲۶	یک دیواره‌ی آتش بین هر دو شبکه‌ای با سطوح مختلف اعتماد قرار می‌گیرد.	
۱۲۷	پشتیبان پیکربندی دیواره‌ی آتش روی شبکه‌ای که بوسیله‌ی آن دیواره‌ی آتش محافظت می‌شود، ذخیره نمی‌شود.	
۱۲۸	ماتریسی از کاربردهای شبکه با هدف مدیریت هدفمند راهبر شبکه، نگهداری می‌شود.	
۱۲۹	سیاست‌های دیواره‌ی آتش حداقل ۳ ماه یکبار رسیدگی و بازبینی می‌شود.	
۱۳۰	آخر همه‌ی قوانین، قانون رد همه‌ی ترافیک نوشته می‌شود و همه‌ی ترافیک برمبنای آن توسط دیواره‌ی آتش جلوگیری می‌شود. مگر اینکه یک قانون خاص اجازه‌ی عبور یک نوع از ترافیک را بدهد.	
۱۳۱	جهت جلوگیری از خدمت به حداقل تعداد ممکن از پروتکل‌ها از مبدا به مقصد اجازه‌ی کار داده می‌شود.	
۱۳۲	جهت جلوگیری از نگاشت شبکه و قوانین دیواره‌ی آتش معین، اجازه‌ی ورود پیام‌های	

بند	توصیه امنیتی	√
	منقضی شده‌ی ICMP[۱۰۵] داده نمی‌شود.	
۱۳۳	از دسترسی ورود به درگاه‌های ۱۳۵، ۱۳۷، ۱۳۸، ۱۳۹، ۴۴۵ و ۳۳۸۹ جلوگیری می‌شود مگر برای سامانه‌های خاص.	
۱۳۴	آدرس IP عمومی فقط در جاهای موردنیاز بکار برده و در جاهای دیگر از ترجمه‌ی نشانی شبکه (NAT[۱۰۶]) و ترجمه‌ی نشانی درگاه (PAT[۱۰۷]) استفاده می‌شود.	
	مسیریاب‌ها و سوئیچ‌ها	
۱۳۵	به منظور محدود کردن ارتباطات بین شبکه‌ها، فهرست های کنترل دسترسی[۱۰۸] (ACLs) پیاده‌سازی می‌شوند.	
۱۳۶	تمامی کلمه‌های عبور ذخیره شده بر روی دستگاه رمزنگاری شده‌است.	
۱۳۷	برای احرازهویت پیشخوان‌های[۱۰۹] مدیریت مسیریاب، از ورود عمومی به سامانه‌ها استفاده نشده است.	
۱۳۸	فقط به آدرس‌های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه‌ها داده می‌شود.	
۱۳۹	تمامی ارتباطات بین پیشخوان مدیریت و مسیریاب‌ها رمزنگاری می‌شود.	
۱۴۰	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	
۱۴۱	حداقل ۲ حساب غیرعمومی[۱۱۰] که دارای امتیازات راهبری[۱۱۱] هستند ساخته می‌شود.	

[۱۰۵] Internet Control Message Port
[۱۰۶] Network Address Translate
[۱۰۷] Port Address Translate
[۱۰۸] Access Control Lists
[۱۰۹] Console

بند	توصیه امنیتی	√
۱۴۲	مسیریاب‌هایی که به شبکه‌های خارجی متصل هستند ، هر ۳ ماه یکبار و مسیریاب‌هایی که به شبکه‌های خارجی متصل نیستند ، هر ۶ ماه یکبار تعمیر می‌شوند.	
۱۴۳	تمامی گزارش‌های مسیریاب به منظور ذخیره‌سازی و تحلیل اتفاقات، به یک کارگزار گزارش-گیری اختصاصی ارسال و این گزارش‌ها حداقل ۳۰ روز نگه‌داری می‌شوند.	
۱۴۴	تمامی احرازهویت‌های راهبردی به دستگاه از طریق یک کارگزار احرازهویت مرکزی مثل RADIUS انجام می‌پذیرد.	
۱۴۵	سوئیچ‌ها قادر به فراهم کردن درگاه‌های SPAN به منظور ثبت و تحلیل ترافیک تولید شده هستند.	
۱۴۶	خدمات مدیریتی غیرضروری (http، indent و ...) و خدمات کنترلی غیرضروری (bootp، CDP، خدمات کوچک TCP/UDP و ...) غیرفعال شده‌اند.	
۱۴۷	گزارش‌گیری فعال و کارگزاری برای گزارش‌گیری تخصیص داده می‌شود.	
۱۴۸	درگاه‌های سوئیچ به طور پیش‌فرض غیرفعال هستند و به VLANهای مهمان/محدود تنظیم شده‌اند.	
۱۴۹	برای هر درگاه سوئیچ یک آدرس MAC تخصیص داده می‌شود.	
۱۵۰	اجازه جعل هویت[۱۱۲] آدرس‌های IP شبکه‌های خارجی داده نمی‌شود.	
مسیریاب مرزی با فهرست کنترل دسترسی		
۱۵۱	مسیریاب‌های مرزی افزونه و همچنین مسیرهای افزونه به منظور حذف خرابی‌های تک‌نقطه-	

[۱۱۰] Non-Generic Account

[۱۱۱] Administrative Privileges

[۱۱۲] Spoofing

بند	توصیه امنیتی	√
	ای در گلوگاه‌ها مورد استفاده قرار می‌گیرند.	
۱۵۲	از ACLهای پیش‌فرض به منظور حفاظت از آدرس‌های IP و درگاه‌هایی که آسیب‌پذیر شناخته می‌شوند استفاده می‌شود.	
۱۵۳	پروتکل‌هایی که معمولا برای مدیریت سیستم به‌کار می‌روند (مثل SSH) در مرزها از آدرس-های IP خارجی شناخته شده محافظت می‌کنند.	
۱۵۴	تغییر مداوم و دوره‌ای رویه‌های مدیریتی ACLها را به صورت منظم بازبینی، اضافه و یا حذف می‌کنند.	
۱۵۵	هر پروتکل و یا هر نوع ترافیکی که توسط سیاست‌های امنیتی سازمان‌ها ممنوع شده‌اند توسط پالایش‌گر بسته‌های مسیریاب مرزی مسدود می‌شوند.	
	سوئیچ‌های LAN	
۱۵۶	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	
۱۵۷	فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه ها داده می‌شود.	
۱۵۸	تمامی رمز عبورهای ذخیره شده بر روی دستگاه رمزنگاری شده‌اند.	
۱۵۹	برای احرازهویت پیشخوان‌های مدیریت مسیریاب، از ورود عمومی به سامانه‌ها استفاده نشده است.	
۱۶۰	سوئیچ‌ها هر دو سال یک‌بار تعمیر و نگهداری و تمامی درگاه‌های بدون استفاده سوئیچ به وضعیت خاموش تنظیم می‌شوند.	
۱۶۱	تمامی گزارش‌های مسیریاب به منظور ذخیره‌سازی و تحلیل اتفاقات، به یک کارگزار گزارش-	

بند	توصیه امنیتی	√
	گیری اختصاصی ارسال و حداقل ۳۰ روز نگه‌داری می‌شوند.	
۱۶۲	پیکربندی VLAN Trunking بر روی درگاه‌هایی از سوئیچ که نیازی به این پیکربندی ندارند غیرفعال شده است.	
۱۶۳	به هنگام استفاده از trunking بر روی درگاه‌های شبکه، پروتکل trunking تعیین می‌شود و به سوئیچ‌ها اجازه داده نمی‌شود تا با پروتکل‌های trunking تبادل اطلاعات کنند.	
۱۶۴	از پل زدن بین دو یا چند VLAN ممانعت می‌شود. اگر نیازی به برقراری ارتباط بین VLANها باشد یک سوئیچ لایه ۳ پیاده‌سازی شده و مسیریابی فعال می‌گردد.	
	شتاب‌دهنده‌ی پهنای‌باند[۱۱۳]/دستگاه‌های اولویت‌بندی	
۱۶۵	تمامی کلمه‌های عبور ذخیره شده بر روی دستگاه رمزنگاری شده‌است.	
۱۶۶	برای احرازهویت پیشخوان‌های مدیریت مسیریاب، از ورود عمومی به سامانه‌ها استفاده نمی-شود.	
۱۶۷	فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه ها داده می‌شود.	
۱۶۸	تمامی ارتباطات بین پیشخوان مدیریت و شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی رمزنگاری می‌شوند.	
۱۶۹	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	
۱۷۰	حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده است.	
۱۷۱	شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی که به شبکه‌های خارجی متصل هستند	

[۱۱۳] Bandwidth Accelerators/Prioritization Devices

بند	توصیه امنیتی	√
	هر ۳ ماه یکبار تعمیر و نگهداری می‌شوند.	
۱۷۲	شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی که به شبکه‌های خارجی متصل نیستند، هر ۶ ماه یکبار تعمیر و نگهداری می‌شوند.	
	دستگاه‌های متمرکز کننده مودم	
۱۷۳	تمامی رمز عبورهای ذخیره شده بر روی دستگاه رمزنگاری شده‌است.	
۱۷۴	برای احرازهویت پیشخوان‌های مدیریت مسیریاب، از ورود عمومی به سیستم‌ها استفاده نمی‌شود.	
۱۷۵	فقط به آدرس های IP داخلی مجاز اجازه دسترسی به مدیریت دستگاه‌ها داده می‌شود.	
۱۷۶	تمامی ارتباطات بین پیشخوان مدیریت و شتاب‌دهنده‌ی پهنای باند/دستگاه‌های اولویت‌بندی رمزنگاری می‌شوند.	
۱۷۷	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	
۱۷۸	حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده است.	
۱۷۹	مسیریاب‌هایی که به شبکه‌های خارجی متصل هستند ، هر ۳ ماه یکبار تعمیر و نگهداری می‌شوند.	
۱۸۰	مسیریاب‌هایی که به شبکه‌های خارجی متصل نیستند ، هر ۶ ماه یکبار تعمیر و نگهداری می‌شوند	
۱۸۱	تمامی درگاه‌هایی از مودم که استفاده نشده‌اند، از کار انداخته می‌شوند.	
۱۸۲	قبل از آن‌که به کاربران اجازه دسترسی داده شود، به گونه‌ای مطلوب احراز هویت می‌شوند.	

بند	توصیه امنیتی	√
۱۸۳	کاربران مودم فقط می‌توانند به سامانه‌هایی دسترسی پیدا کنند که بدان‌ها برای اهداف تجاری نیاز دارند.	
فیلتر کننده های مبتنی بر محتوی [۱۱۴]		
۱۸۴	فیلترکننده‌های مبتنی بر محتوی از ترکیبی از «فهرست‌های سیاه» و «فهرست‌های سفید» استفاده می‌کنند.	
۱۸۵	فیلترکننده‌های مبتنی بر محتوی با توجه مشاوره‌های امنیتی فروشنده اصلاح و نگهداری می‌شوند.	
۱۸۶	امضاهای پالایش‌گرهای محتوا به صورت روزانه به‌روزرسانی می‌شوند.	
۱۸۷	گزارشی شامل فعالیت‌های پالایشی به صورت روزانه تولید و توسط مدیر IT بازبینی می‌شوند.	
آنتی‌ویروس‌ها		
۱۸۸	دروازه‌های آنتی‌ویروس به منظور پایش ترافیک وب و ایمیل ورودی و خروجی برای تشخیص فعالیت‌های مشکوکی که دلالت بر وجود یک ویروس یا بدافزار دارند پیاده‌سازی شده است.	
۱۸۹	اتصالات شبکه‌ای از سوی ایستگاه‌های‌کاری[۱۱۵] به شبکه‌های داخلی و اینترنت مسدود می‌شوند تا از گسترش و فعالیت بدافزارها ممانعت شود.	
نقاط دسترسی بی‌سیم		
۱۹۰	پیشخوان راهبری از طریق شبکه رادیویی بی‌سیم قابل دسترسی نیستند.	

[۱۱۴] Content Filters

[۱۱۵] Workstations

بند	توصیه امنیتی	√
۱۹۱	نقاط دسترسی بی‌سیم در پاسخ به هشدارهای محصول که توسط فروشنده سخت‌افزار منتشر می‌شوند تعمیر و نگهداری می‌شوند.	
۱۹۲	تمامی کارخواه‌های[۱۱۶] از رمزنگاری‌های قوی استفاده می‌کنند.	
۱۹۳	تمامی شبکه‌های بی‌سیم به یک VLAN مجزا ختم می‌شوند.	
۱۹۴	از POA یا مسئول آن برای نصب یک AP مجوز گرفته می‌شود.	
۱۹۵	به منظور آگاهی ISO، قبل از نصب و راه‌اندازی نقاط دسترسی بی‌سیم که برای پردازش و ارسال داده‌های طبقه‌بندی شده مورد استفاده قرار خواهد گرفت با POA همکاری می‌شود.	
۱۹۶	دستگاه‌ها از ارتقاء میان افزار پشتیبانی می‌کنند به گونه‌ای که بسته‌های امنیتی به محض در دسترس بودن نصب می‌شوند.	
۱۹۷	دستگاه‌ها از ملزومات محافظت از هر سطحی از اطلاعات و طبقه‌بندی سیستم پشتیبانی می‌کنند.	
۱۹۸	تمامی کاربردهای متصل به شبکه‌های دانشگاهی ثبت می‌شوند.	
۱۹۹	پشتیبانی[۱۱۷] از تمامی نرم‌افزارها، راهنمای نصب، و رویه‌های لازم برای پشتیبانی از شبکه‌های بی‌سیم جمع‌آوری و ذخیره می‌شوند.	
۲۰۰	تمامی کاربردهای به دور از دسترس نصب می‌شوند تا از حملات مهاجمینی که می‌توانند یک نقطه دسترسی تقلبی ناامن را به جای نقطه دسترسی حفاظت شده جایگزین کنند، ممانعت شود.	

[۱۱۶] Clients

[۱۱۷] Backup

بند	توصیه امنیتی	√
۲۰۱	ارزیابی از ریسک می‌شود تا از پیکربندی صحیح دستگاه‌های بی‌سیم و امنیت اطلاعات اطمینان حاصل شود.	
۲۰۲	محدوده‌ی نقاط دسترسی بررسی و اطمینان حاصل می‌شود که محدوده پوشش‌دهی فقط دستگاه‌های نیازمند دسترسی را شامل می‌شود.	
۲۰۳	عملیات راه‌اندازی مجدد نقاط دسترسی فقط به هنگام ضرورت انجام می‌پذیرد، و فقط توسط افراد مجاز ممکن می‌باشد.	
۲۰۴	ارتباطات بی‌سیم از دسترسی مستقیم به سامانه‌هایی که بر روی شبکه سیمی قرار دارند چه به صورت فیزیکی و چه به صورت نرم‌افزاری جدا شده است.	
۲۰۵	انتشار امواج رادیویی در خارج از منطقه مورد نیاز با استفاده از آنتن‌های قابل هدایت کاهش داده می‌شود.	
۲۰۶	SSID نقاط دسترسی تغییر داده شده است.	
۲۰۷	همه‌پخشی مشخصه SSID غیرفعال می‌شود به گونه‌ای که SSID کارخواه باید با SSID نقطه دسترسی منطبق باشد.	
۲۰۸	رشته کاراکتری SSID از هیچ نامی که بتواند با نام دانشگاه تداعی شود استفاده نمی‌کند.	
۲۰۹	تمامی دستگاه‌ها دارای رمز عبورهای راهبری قوی می‌باشند.	
۲۱۰	تمامی پیکربندی‌های پیش‌فرض غیرضروری تغییر کرده است.	
۲۱۱	تمامی پروتکل‌های غیرضروری بر روی دستگاه بی‌سیم غیرفعال شده است.	
۲۱۲	دستگاه بی‌سیمی که از گزارش‌گیری پشتیبانی می‌کند، روشن است و گزارش‌ها را به طور مرتب بازبینی می‌کند.	

بند	توصیه امنیتی	√
۲۱۳	نقاط دسترسی به هنگامی که از آن‌ها استفاده نمی‌شود خاموش هستند.	
۲۱۴	هر نقطه دسترسی غیرمجازی که به شبکه دانشگاه متصل هستند غیرفعال و حذف می‌شوند.	
۲۱۵	ترافیک مدیریتی مربوط به دستگاه بی‌سیم بر روی یک زیرشبکه‌ی اختصاصی و مجزا می‌باشد.	
۲۱۶	به هنگام راهبری از راه دور دستگاه‌های بی‌سیم، از مدهای امن انتقال مثل HTTPS و SSH استفاده می‌شود.	
	دستگاه‌های **VPN**	
۲۱۷	به مدیریت دستگاه VPN اجازه داده می‌شود تا فقط به آدرس‌های IP داخلی مجاز دسترسی پیدا کند.	
۲۱۸	دستگاه‌های VPN در پاسخ به هشدارهای محصول که توسط فروشنده سخت‌افزار یا نرم‌افزار منتشر می‌شوند تعمیر و نگهداری می‌شوند.	
۲۱۹	دستگاه‌های VPN در یک منطقه حائل (بخشی از IP شبکه) اختصاصی قرار می‌گیرند.	
۲۲۰	به کاربران VPN اجازه داده می‌شود که صرفا به سامانه‌هایی که برای دسترسی به اهداف تجاری بدان‌ها نیاز دارند متصل شوند.	
	کارگزارهای نماینده‌ی وب	
۲۲۱	به مدیریت کارگزار نماینده اجازه داده می‌شود تا فقط به آدرس‌های IP داخلی مجاز دسترسی پیدا کند.	
۲۲۲	هر نماینده صرفا طوری پیکربندی می‌شود که فقط اجازه جریان ترافیک در یک جهت را بدهد.	

بند	توصیه امنیتی	√
۲۲۳	نماینده‌ها در پاسخ به هشدارهای محصول که توسط فروشنده سخت‌افزار یا نرم‌افزار منتشر می‌شوند تعمیر و نگهداری می‌شوند.	
۲۲۴	تمامی کاربران نماینده قبل از دسترسی به اینترنت یا سایر خدمات مجاز احراز هویت می‌شوند.	
	دروازه‌ی VoIP	
۲۲۵	به مدیریت دروازه VoIP اجازه داده می‌شود تا فقط به آدرس‌های IP داخلی مجاز دسترسی پیدا کند.	
۲۲۶	تمامی ترافیک دسترسی مدیریت باید رمزنگاری شوند.	
۲۲۷	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	
۲۲۸	حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده است.	
۲۲۹	اجازه دسترسی خارجی به ثبات[۱۱۸] کاربر داخلی که در سامانه VoIP پیکربندی شده است داده نمی‌شود.	
۲۳۰	دروازه‌های VoIP در پاسخ به هشدارهای محصول که توسط فروشنده دروازه‌ها منتشر می‌شوند تعمیر و نگهداری می‌شوند.	
۲۳۱	نشست‌های VoIP رمزنگاری می‌شوند.	

[۱۱۸] Register

بند	توصیه امنیتی	√
سیستم تشخیص نفوذ / جلوگیری از نفوذ[۱۱۹] (IDPS)		
۲۳۲	مدیریت دسترسی فقط به آدرس‌های IP داخلی مجاز محدود می‌شود.	
۲۳۳	تمامی ارتباطات بین پیشخوان مدیریت و دستگاه رمزنگاری می‌شوند.	
۲۳۴	واسط‌های شبکه که برای پایش و جمع‌آوری ترافیک شبکه مورد استفاده قرار می‌گیرند با یک آدرس IP پیکربندی نمی‌شوند.	
۲۳۵	کلمه‌های عبور سامانه دارای حداقل ۸ کاراکتر و ترکیبی از کاراکترهای با حروف بزرگ و کوچک، اعداد و کاراکترهای مخصوص دیگر می‌باشند.	
۲۳۶	حداقل ۲ حساب غیرعمومی که دارای امتیازات راهبردی هستند ساخته شده است.	
۲۳۷	دستگاه‌ها در پاسخ به سیستم‌عامل و هشدارهای محصول که توسط فروشنده‌های مربوطه منتشر می‌شوند تعمیر و نگهداری می‌شوند.	
۲۳۸	به روز رسانی دوره‌ای امضاء از سوی فروشنده قابل دسترس می‌باشد و بین انتشار امضاءهای جدید توسط فروشنده و دریافت آن‌ها توسط IDPS بیش از یک هفته فاصله نمی‌افتد.	
۲۳۹	یک رویه‌ی مدیریتی انجام تغییرات که به طور خاص برای IDPS طراحی شده است توسعه و با توجه به به‌روزرسانی‌های امضاءهای جدید اعمال می‌گردند.	
۲۴۰	ترافیک پایش شده از پهنای باند IDPS و درگاه سوئیچ بیشتر نمی‌شود.	
۲۴۱	IDPS قادر است تا بسته‌های جدا ازهم مربوط به سیستم‌عامل‌های مختلف را به هم متصل کند.	

[۱۱۹] Network Intrusion Detection/Prevention Systems

بند	توصیه امنیتی	√
۲۴۲	IDPS قادر به گزارش‌گیری بر روی یک سامانه پایگاه داده می‌باشد.	
۲۴۳	IDPS قابلیت تنظیم قوانین و سفارشی‌سازی آن‌ها را دارد.	
۲۴۴	یک رویه‌ی مدیریتی انجام تغییرات توسعه و با توجه به تنظیمات صورت گرفته برای قوانین اعمال می‌گردد.	
۲۴۵	سیستم‌های IDPS دارای چندین کارت واسطه‌ی شبکه می‌باشند تا یکی از آن‌ها بتواند در برابر سایر سامانه‌ها نامرعی[۱۲۰] و یا فقط قابل خواندن باشد.	
۲۴۶	جایابی IDPS بر روی یک شبکه خاص بر مبنای طبقه‌بندی اطلاعات بر روی آن شبکه صورت می‌گیرد.	
۲۴۷	حسگرهای IDPS بر روی هر نوع شبکه‌ای که احتمال درز اطلاعات در آن می‌رود قرار دارد.	
۲۴۸	مجموع پهنای باند تمامی درگاه‌ها نباید از پهنای باند درگاه SPAN فراتر رود.	
۲۴۹	سامانه‌ها و انواع ترافیکی که هر IDPS پایش می‌کند شناخته شده است.	
۲۵۰	قوانینی که برای آن‌ها سیستم/کاربرد مرتبطی وجود ندارد غیرفعال می‌شود و پهنای باند با ارزش IDPS از هدر رفتن حفظ می‌شود.	
۲۵۱	در مورد سامانه‌های تشخیص متن‌باز مثل Snort، به هنگام اجرای IDPS بر روی سیستم عاملی که بسته‌ها را مجددا بازبینی می‌کند احتیاط‌های لازم صورت نمی‌گیرد.	
۲۵۲	از هاب برای دسترسی IDPS به ترافیک استفاده نمی‌شود.	
۲۵۳	حسگرهای IDPS دارای واسطی بر روی یک شبکه مدیریتی که از ترافیک تولیدی مجزا است می‌باشند.	

[۱۲۰] Invisible

بند	توصیه امنیتی	√
۲۵۴	واسط استماع[۱۲۱] بر روی شبکه فقط خواندنی می‌باشد تا از بروز حمله بر روی IDPS ممانعت شود.	

[۱۲۱] Listening