منتجات شركه NAAD

:::::::: بسيطة، لكنها غير قابلة للاختراق ::::::::

- مجموعة منتجات أمن الشبكة NAAD تقدم مستوى جديدًا من أمن الاتصالات.
- تـم تصميـم هـذه المنتجـات و بناؤهـا بالاخـص لربـط الشـبكات الحساسـة فـي المؤسسـات التي تحافـظ على البنيـة التحتيـة الحيويـة للبلد.

- تتميـز هـذه المنتجـات، إلى جانب إنشـاء الأمـان باسـتخدام الهندسـة المعمارية الفريـدة الخاصة بهـا التـي يمكـن أن تجعـل اختـراق الشـبكة المؤسسـية تقريبًـا مسـتحيلاً، بواجهـة مسـتخدم بسـيطة للغايـة، وتثبيتهـا وتشـغيلها فـي أي شـبكة معقـدة يكـون سـهلاً للغاية.

- تـم وضـع DENA و DAMAVAND فـي فئـة منتجـات أمـان بوابـة الشـبكة (Gateway)، بهـدف منـع المهاجميـن مـن الاختـراق إلـى شـبكة المؤسسـة ومنع تسـرب المعلومات الحساسـة للمؤسسـة ، حيـث يتصـل الشـبكات المحليـة المتنوعة للمؤسسـة بمسـتويات أمـان مختلفة.

مــزود المنتجــات القائمــة علــى المعرفـة فـي مجـال أمن الشـبكات

تأمين أمن البنية التحتية الحساسة للمؤسسات

مناسـبة لتوسـيع الشـبكة فجـوة الهـواء (Air Gap) والاتصـال عـن بعـد.

لماذا منتجات NAAD غیر قابلة للاختراق؟

- المیـزة الرئیسـیة لمنتجـات أمـان شـبکة NAAD مقارنـة بالمنتجـات الأخـرى الموجـودة فـي السـوق، هـي تنفیـذ الأجـزاء الحساسـة علـى هـذه المنتجـات، بمـا فـي ذلـك جـزء التعمیة فـي شـکل عتادیـه و علـى FPGA. نظـرًا لهذا، هـذه المنتجـات تقـاوم العدیـد مـن الهجمـات التي تسـتهدف أنظمـة البرامـج، وتوفر أیضًـا إمکانیة تنفیـذ طلبات الخوارزمیـات المخصصة للمؤسسـات.

- بالإضافـة إلـى جـزء العتـادی، یوجـد فـي اللـب الرئیسـي للمنتج معالـج لتنفیـذ البروتوکـولات المعقـدة ، والتي یتم تنفیـذ البرنامـج علیهـا. مـن أجـل الحفـاظ علی مسـتوی عـالٍ مـن الأمان في هـذا الجـزء ، یتـم اسـتخدام معماریه bare-metal. فـي هـذا النـوع مـن التصمیـم ، لا یتـم اسـتخدام أي نظـام تشـغیل تقلیـدي ، و یتـم تنفیـذ البرنامج مباشـرة عـن طریـق إعـادة تنفیـذ أجـزاء صغیرة مـن نظام التشـغیل.

- تسـتفید البنیـة المسـتخدمة فـي منتجـات أمـان شـبکة NAAD ، عبـارة عـن مزیـج مـن عتـاد والبرامـج فـي نفـس الوقـت (hardware-software codesign). مـع مزیـج مـن نقـاط القـوة لـکل منهـا ، فقـد خلقت منتجـات لا یمکن اختراقهـا. تتمثـل السـمات الرئیسـیة لهـذه البنیـة فـي اسـتخدام FPGA فـي تصمیـم العتـاد و المعمـاری bare-metal، ممـا یقلـل کثیـر مـن مخاطـر الاختـراق و الضعـف.

فئتان من المنتجات لحاجتین مختلفتین

۱. فئه منتجات DAMAVAND:

- منتجـات هـذه الفئـة مناسـب للاسـتخدام فـي المؤسسـات أو مراکـز البیانـات (Enterprise) و لدیهـا القـدرة علـى إنشـاء اتصـال لعـدة أشـخاص فـي نفـس الوقـت.

۲. فئه المنتجات DENA:

- یشـبه هـذا النـوع مـن المنتجـات منتجـات Damavand مـن حیـث الوظیفـة ، إلا أنـه ذو أبعـاد أصغـر ومناسـب للاسـتخدام الشـخصي(personal) فـي شـکل محمـول أو ثابـت.

مشاكل البنية التحتية الحالية للمنظمات:

١. التكلفة العالية لتصلب الشبكة بطرق العزل(isolation) / فجوة الهواء (air gap):

بعض البنى التحتية الحالية للمراكز الحساسة في العالم منفصلة ماديًا عن البيئة. تُستخدم الألياف الداكنة(dark fiber) والروابط المخصصة(point-to-point) في طرق العزل الشائعة. هذه الأساليب بها بعض المشاكل ، بما في ذلك ارتفاع مصاريف الصيانة و مصاريف التوسعة العالية (المالية والوقت). في بعض الأحيان يخلقون أيضًا مشاكل معقدة لأسباب جغرافية ومدنية.

إذا كانت هذه البنى التحتية تستخدم طرقًا عالية الأمان قائمة على العتاد ، فسيكون من الممكن إضافة شبكات جديدة بتكلفة أقل بكثير.

٢. وجود أنواع مختلفة من الثغرات الأمنية في تقوية البرامج (MPLS ، خادم VPN ، إلخ):

يؤدي التصلب من خلال أساليب التطبيقات البرمجية إلى خلق نقاط ضعف ، بما في ذلك الثغرات الأمنية في سلسلة توريد البرامج في النظام ، والتي تعد سببًا للعديد من الهجمات الإلكترونية.

٣. استحالة الاتصال عن بُعد للموظفين المتخصصين في المنظمة:

في بنية البنية التحتية القائمة على العزلة المادية ، لا يمكن الاتصال بشبكات المؤسسة عن بُعد. على سبيل المثال ، يحتاج كبار خبراء المنظمة إلى الوصول إلى الشبكة الرئيسية في المناسبات الحساسة خلال غير ساعات العمل من خارج المكتب. تم حل هذه الحاجة بمساعدة مجموعة المنتجات الفردية (Dena).

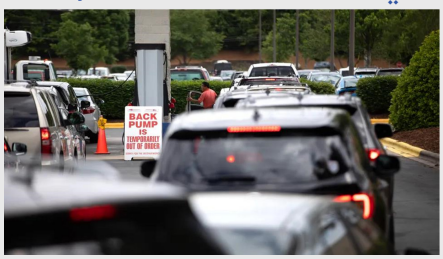
٤. صعوبة استخدام المنتجات الأمنية:

تشتري بعض المؤسسات منتجات لتأمين شبكتها الخاصة ، لكن لا تستخدمها بسبب الدعم غير المناسب و صعوبة التكوين. تم أخذ هذه المشكلة بعين الاعتبار في تصميمات تجربة المستخدم لمنتجات NAAD. لهذا السبب ، تم استخدام واجهات مستخدم بسيطة مع إمكانية التكوين السريع.

٥. إمكانية وجود باب خلفي في المنتجات غير الآمنة:

أحد مخاوف المنظمات التي تستخدم أنظمة أمان غير موثوق بها هو وجود طريقة اختراق داخل الأجهزة من قبل الشركة المصنعة للمعدات نفسها(backdoor). إن استخدام أنظمة الأمان الآمنة يلغي هذا القلق.

هجوم على شبكة إمدادات الوقود لخطوط الأنابيب الاستعمارية في الولايات المتحدة عام ٢٠٢٠



في هذا الهجوم ، تم تعطيل نظام تزويد الوقود في جنوب شرق الولايات المتحدة لعدة ساعات. حدث هذا الهجوم من خلال اختراق شبكة المنظمة وضعف الشبكة الداخلية. الأمان المقترح عن طريق العتاديات مناسب تمامًا وآمن لهذا النوع من الهجوم.

هجوم على شبكة الوقود الإيرانية

في هذا الهجوم ، لم يكن نظام الوقود الذكي متاحًا لفترة من الوقت ، مما أدى إلى تغطية إعلامية كبيرة. في العديد من أساليب الهجوم، تكون الخطوة الأولى هي التسلل إلى الشبكة الداخلية للمؤسسة. إذا كان النظام يمنع الاختراق، فإنه يوقف المهاجم في الخطوة الأولى.

ثغرات يوم الصفر(zero day):

تتسبب هذه الأنواع من الثغرات الأمنية في حدوث أخطر الهجمات على الأنظمة. Zero-day هو نوع من ثغرات البرامج التي لم يكن صانع البرامج على دراية بها أو لم ينجح في حلها. في كل عام ، يتم تنفيذ عدد كبير من عمليات الاستغلال التي تسببها ثغرات يوم الصفر على الأنظمة وتسبب ضررًا كبيرًا لها.

يتناسب احتمال العثور على نقاط الضعف هذه مع حجم البرنامج ، ولهذا السبب ، فإن المعمارى bare-metal في منتجات NAAD أكثر أمانًا ضد هذه الهجمات.

لماذا يجب علينا استخدام منتجات NAAD؟

۱. التكلفة المنخفضة والتوسع السريع للشبكة الداخلية:

لإضافة فرع جديد للمؤسسة وتوصيله بالشبكة الداخلية ، يكفي توصيل الفرع الجديد بالشبكة الداخلية عن طريق تثبيت منتج Damavand كبوابة وتنفيذ إعداداته الأولية.

۲. منتجات أمنية ذات ابتكار في الهندسة المعمارية:

يعتمد أمان منتجات NAAD على بنيتها وطريقة تصميمها ، وهي تختلف اختلافًا جوهريًا عن طرق الأمان الأخرى.

۳. دعم وأمن مستمر للمنتجات من قبل فريق الخبراء:

يقوم فريق المراقبة الأمنية التابع لشركة NAAD باستمرار بعملية اختبار الصلابة والأمان ، وهم يضمنون أمان المنتج أثناء الاستخدام

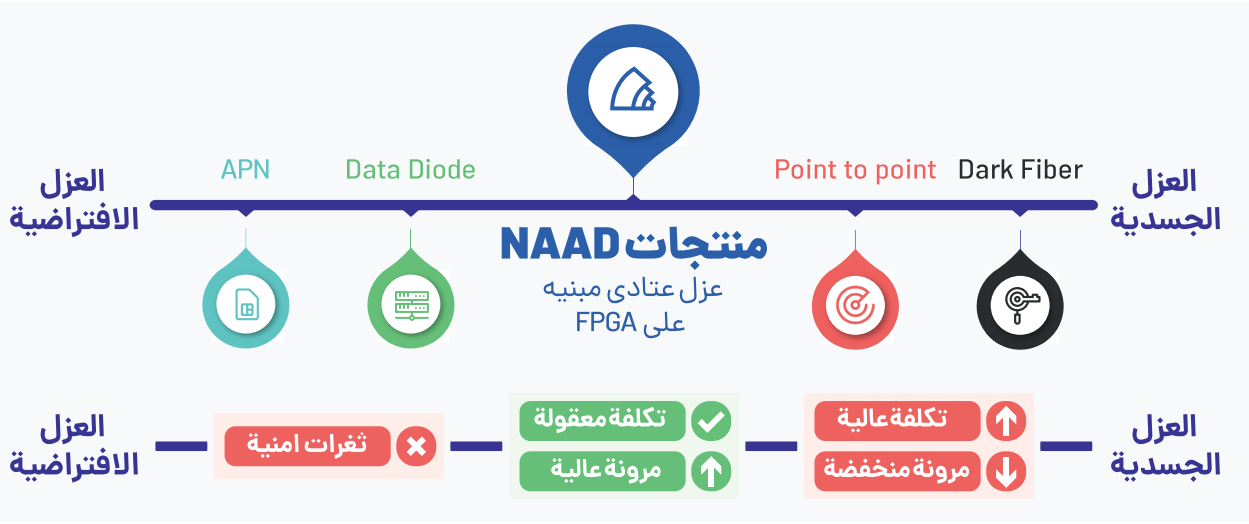
٤. التكوين البسيط (plug and play):

تصميم واجهات المستخدم بطريقة توفر للمستخدم إمكانية الإعداد السريع وضبط الجهاز في ظروف مختلفة.

٥. إمكانية الاتصال عن بعد للموظفين المتخصصين في المنظمة:

باستخدام Dena جنبًا إلى جنب مع منتج Damavand ، من الممكن أن يكون لديك اتصال عن بعد لبعض الموظفين دون تقليل أمان الشبكة الرئيسية.

أنواع طرق عزل الشبكة:



تنقسم الطرق الحالية لعزل الشبكات الحساسة إلى فئتين: العزلة المادية والعزلة الافتراضية. يتم تصنيف المنتجات مثل خوادم VPN ، التي تستخدم نظام تشغيل Linux في الجزء الرئيسي من معالجتها ، على أنها عزل افتراضي. هذه المنتجات ليست في مأمن من نقاط الضعف في نظام التشغيل والحزم التابعة الأخرى ، حتى لو قامت بتأمين برامجها الأصلية.

من ناحية أخرى ، يتم تصنيف الأساليب مثل استخدام dark fiber أو point-to-point لأمن الشبكة في فئة العزل المادي.

كما ذكرنا ، فإن هذه الأساليب تتكبد الكثير من التكاليف في توسيع والحفاظ على الوصول إلى شبكة المؤسسة. مشكلة أخرى هي عدم المرونة والانقطاع في سير عمل المنظمة.

تقدم منتجات NAAD ، المصنوعة بهندسة خاصة ، طريقة مختلفة للعزل في طبقة العتاديات ، والتي يمكن أن تكون بديلاً مناسبًا للعزل المادي. تعتمد هذه المنتجات، التي تحتوي نواة آمنه بمساعده البرمجيات بهندسه bare-metal و عتاد FPGA.

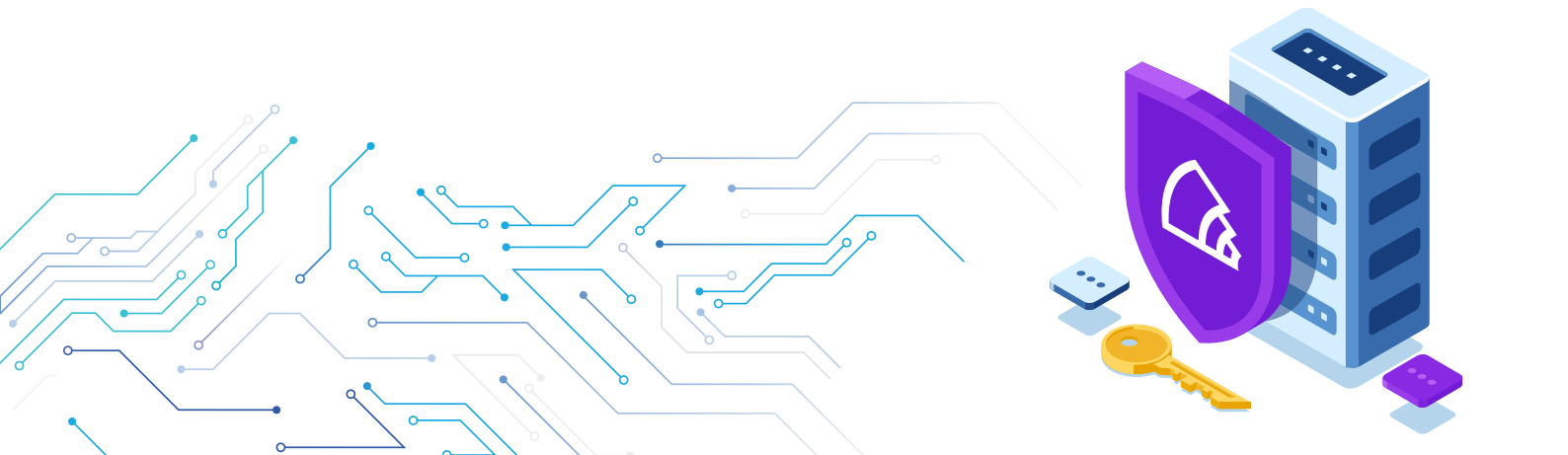
Damavand

Family		200 Mbps	1 Gbps		
Type			Base	Standard	Premium
Tunneling	Encrypted Trafic	200 Mbps	1 Gbps	1 Gbps	1 Gbps
	PPS	16 Kpps	1 Mpps	1 Mpps	1 Mpps
	Simultaneous instances	120	120	120	240
	tun support	Yes	Yes	Yes	Yes
	tap support	Yes	Yes	Yes	Yes
	NAT traversal	Yes	Yes	Yes	Yes
	Handshake StaticKey	Yes	No	No	Yes
Networking	VLAN	Yes	No	No	Yes
	External Interface	1x GigEth - RJ45			
	Internal Interface	1x GigEth - RJ45			
HSM	Certificates	Yes	No	Yes (max.150)	Yes (max.300)
	2 Factor Authentication	Yes	Yes	Yes	Yes
	PKCS11	Yes	Yes	Yes	Yes
	Side channel security	Yes	Yes	Yes	Yes
	Cryptographic Algorithms	RSA 2048/4096 AES GCM 256 ECDH			
	Custom ECC Curves	No	No	No	No
	Custom Algorithms	No	To be negotiated.		
Encrypted Flash		Yes	Yes	Yes	Yes
Firmware integrity check		Yes	Yes	Yes	Yes
Zeroization		Yes	Yes	Yes	Yes
Internal RTC		Yes	Yes	Yes	Yes
Audit Log		No	No	No	To be negotiated
Monitoring		No	No	No	To be negotiated

Dena Desktop

Dena Portable

Type		Dena Desktop	Dena Portable
Baremetal architecture (very small OS+ Software foot print)		Yes	Yes
Tunneling	Encrypted Traffic Throughput	16 Mbps	16 Mbps
	Simultaneous tunnel instances	1	1
	Layer 3 tunneling (tun)	Yes	Yes
	NAT traversal	Yes	Yes
	Tunnel Cryptographic Algoritms	RSA 2048/4096 AES GCM 256 ECDH	
	Post-Quantum security (Handshake static key)	Yes	Yes
	Certificate-based tunnels	Yes	Yes
	2 Factor Authentication	Yes	No
Interfaces	Internal Interface	1* 10/100Eth	3G/4G/LTE
	External Interface	USB	WIFI & USB
Security	Side-Channel security	Yes	Yes
	Custom ECC Curves	No	To be negotiated.
	Custom Algorithms	No	To be negotiated.
Tamper	Encrypted Flash	Yes	Yes
	Firmware integrity check	Yes	Yes
	Internal RTC	Yes	Yes
	Temper Resistant	No	Yes



تأسس مبتكرو الشريف ذو العقلية الآمنة، NAAD ، من قبل عدد من الزملاء الأكاديميين والباحثين من جامعة الشريف التكنولوجية في عام ٢٠١٤ بهدف تأمين البنى التحتية الحيوية الوطنية.

حتى الآن ، نجحت هذه الشركة في التحرك نحو مهمتها من خلال تأمين البنية التحتية للاتصالات للمنظمات الحساسة في إيران.