



NOX Systems

Security Whitepaper

Version 20.0

Version	Forfatter	Ændringer	Dato
19.0	Christian Tyllesen	NIS2 segment tilføjet	28.05.2024
20.0	Christian Tyllesen	OSDP Kryptering tilføjet	08.07.2024

ARAS Security A/S

+45 7027 4090

info@aras.dk

www.aras.dk

Indholdsfortegnelse

Introduktion til NOX Software releases.....	3
NOX og SIMS, almindelige porte i brug	4
NOX Hardware	5
NOX BUS	5
OSDP BUS.....	5
NOX Centraler i netværk	6
NOX Redundant CPU	6
NOX PC Control.....	6
NOX PC TPA	7
NOX Logger	8
NOX Config	9
NOX SIMS V6.....	10
iNOX & NOX for Android, MacOS	11
NOX SSH.....	12
NOX PCIF (Generel beskyttelse af PC Interface).....	13
NOX Kode politik (betjeningsenheder på NOX BUS)	14
NOX Kort + PIN kode politik (CMx interfaces på NOX BUS).....	14
Dataflow/Båndbredde forbrug.....	15
NIS2 med NOX og SIMS	17

Introduktion til NOX Software releases

EOL Systemsoftware

Software release $\leq R6$ er End-of-life, og er ikke længere supporteret og bliver ikke opdateret fra NOX Systems side.

Det er anbefalet at opdatere NOX CPU'erne til R8 (11.xx) for at sikre nyeste sikkerhedsteknologi, samt fortsat support og opdatering.

Gyldig fra systemversion R7

NOX centrale software er designet til at opfylde de nyeste IT-sikkerhedsstandarder.

Til dette formål er al Datatransmission krypteret (undtagen NOX TIO-enhed), og forbindelsen er autentificeret på netværkslaget.

Derudover skal brugeren autentificere sig over for systemet ved hjælp af en brugerkode eller brugernavn/adgangskode.

Hvis centralenheden med de lagrede data kommer på fremmede hænder, kan de data, der er lagret på CPU'en, ikke udlæses uden gyldig autentificering.

Sikkerhedsforanstaltninger:

- Brug af TLS 1.2
- Beskyttelse mod brute force angreb
- Beskyttelse mod man-in-the-middle-angreb
- Valgfri kundespecifikke certifikater til TLS-godkendelse
- Konfigurationsdata i CPU'en gemmes krypteret
- Systemfiler i CPU'en kontrolleres for gyldighed ved hjælp af kryptering
- PC-applikationer benytter Code Signing

Anbefalinger til højsikkerhedsinstallationer (Klasse 3 og 4)

- Brug af SL4 (godkendelse ved hjælp af brugernavn og adgangskode)
- Brug af en adgangskode til at vise konfigurationen
- Brug af komplekse adgangskoderegler
- Aktivering af kun de nødvendige netværkstjenester i systemet
- Ingen brug af NOX TIO-enheder med kontrolfunktioner (ingen kryptering)
- Begrænsning af Brugerinterfaces til det absolut nødvendige
- Brug af tidsprofiler til at begrænse brugernes gyldighed

NOX og SIMS, almindelige porte i brug

Retning	Applikation	Beskrivelse	Fra	Til	Port	Konfigurerbar	Sikkerhed	Standard indstilling
NOX Indgående								
	NOX Config	Generel System Konfiguration	Software	Central	4322	Nej	Krypteret	Åben
	NOX Config	NOX Loader	Software	Central	6251	Nej	Krypteret	Åben
	NOX Config	Terminal Window	Software	Central	4321	Nej	Krypteret	Åben
	NOX PC Control	Bruger interface for Windows PC	Software	Central	4322	Nej	Krypteret	Åben
	NOX PC TPA	Bruger interface for Touch Skærm m. grafik	Software	Central	4322	Nej	Krypteret	Åben
	NOX SmartPhone App	Bruger interface for SmartPhones og MacOS	Software	Central	4325	Ja	Krypteret	Lukket
	NOX SSH Server	Bruger interface, for simple integrationer	Software	Central	22	Ja	Krypteret	Lukket
	NOX Modbus Server	Integration med HVAC/CTS Systemer	Software	Central	502	Ja	Ingen	Lukket
	NOX SNMP Trap Receiver	SNMP trap modtager fra udvalgte Communities	Software	Central	162	Nej	Ingen	Lukket
	NOX TIO	Bruger interface, Telnet/Tekst beskeder	Software	Central	4001	Ja	Ingen	Lukket
	NOX in Network Configuration	Flere NOX Centraler i samme netværk	UnderCentral	HovedCentral	8981	Nej	Krypteret	Lukket
NOX Udgående								
	NTP	Tidssynkronisering via NTP Server	Central	Service	123	Nej	Ingen	Lukket
	Modbus Client	Integration med HVAC/CTS Systemer	Central	Service	502	Ja	Ingen	Lukket
	SMTP	E-mail udsending direkte fra NOX Central	Central	Service	587	Ja	Krypteret	Lukket
	NOX SmartPhone App	NOX Push notifications: push.noxsystems.com	Central	Service	4324	Nej	Krypteret	Lukket
	NOX TIO	Bruger interface, Telnet/Tekst beskeder	Central	Service	4001	Ja	Ingen	Lukket
	SmartIntego	Trådløse døre til NOX	Central	Gatenode	2101	Nej	Ingen	Lukket
	SIA IP	Alarmtransmission	Central	KC	30001	Ja	Valgfri	Lukket
SIMS Indgående								
	SIMS Client	Klient til styring af SIMS forbundet NOX Centraler	Client PC	SIMS Server	2010	Ja	Krypteret	Åben
SIMS Udgående								
	SIMS Server	Forbindelse til NOX Centraler	SIMS Server	Central	4322	Nej	Krypteret	Åben
	NOX License Server	NOX Systems Licens server: license.noxsystems.com	SIMS Server	Service	8777	Nej	Krypteret	Åben

NOX Hardware

NOX BUS

NOX bussen er af type RS-485 Standard.

NOX bussen benytter obfuskering/sløring af data ved kommunikation mellem CPU og NOX enheder, udviklet af NOX Systems.

Alle beskeder skifter form fra gang til gang de benyttes, og det er derfor meget kompliceret at skulle simulere/emulere en besked, og afspille denne tilbage på NOX bussen.

NOX bussen indgår som en del af NOX systemet, og har ikke nogen indflydelse på IT-infrastrukturen, den udføres som en selvstændig del af selve NOX installationen.

Ved afbrydelse af bussen vil NOX systemet generere en sabotage alarm for alle manglende enheder.

Ved forsøg på manipulation med datapakker vil disse blive ignoreret da de ikke indeholder den korrekte datastruktur.

OSDP BUS

OSDP bussen kan beskyttes med en 128bit AES kryptering, den er valgfri og er ikke valgt som standard.

OBS. kræver NOX System $\geq$ 10.51L (R8) og CMO FW $>$ 30

NOX Centraler i netværk

NOX i netværksforhold, består af 2 eller flere NOX CPU som kommunikerer via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256bit AES kryptering.

Kommunikationen foregår på følgende porte: 8981

Porten er låst og kan ikke ændres.

NOX Redundant CPU

NOX Redundant CPU, består af 2 NOX CPU som kommunikerer via TCP/IP, de er 1 til 1 dubleret, samt deler fysiske busser, således at der ved genstart eller nedbrud af den ene, tager den anden over uden afbrydelser. Al kommunikation mellem primær og sekundær CPU foregår uden kryptering.

Kommunikationen foregår på følgende porte: 8982

NOX PC Control

NOX PC Control er betjeningssoftware som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256bit AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

NOX PC TPA

NOX PC TPA er betjeningssoftware som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256bit AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

NOX Logger

NOX Logger er et lille stykke software som kan køre uafhængigt af NOX Config eller NOX PC Control, egenskaberne for dette program er at opsamle logs i real-time gennem NoxDLL.dll.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85 (**NOX Logger 3.0**)

Fra R7 (Version 10.0) benyttes 256bit AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering. (**NOX Logger 4.0**)

Software kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

NOX Config

NOX Config er konfigurationssoftware som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256bit AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4321, 4322, 6251

Portene er låst og kan ikke ændres.

NOX SIMS V6

SIMS er en Server/Client software løsning for multicentral- og grafisk løsning med mulighed for integration gennem SQL Server. SIMS betyder Security Information Management System.

Server:

Kommunikationen mellem SIMS Server og NOX CPU'er, er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256bit AES kryptering og TLS 1.2 (SSL)

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1) og .NET 4.5

Kommunikationen foregår på følgende porte: 4322, 8777

Portene er låst og kan ikke ændres, hvis der ikke er adgang til port 8777, skal evt. licens opdateringer overføres manuelt.

Client:

Kommunikationen mellem SIMS Client og SIMS Server er beskyttet med en 128 bit AES kryptering.

Software kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1) og .NET 4.5

Kommunikationen foregår kun mod SIMS Serveren på følgende porte: 2010

Port 2010 er anbefalet men kan frit ændres.

iNOX & NOX for Android, MacOS

iNOX og NOX for Android er Smartphone apps som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256bit AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Kommunikationen foregår på følgende porte: 4325

Porten er anbefalet men kan frit ændres.

NOX SSH

NOX SSH er kun SSH Server, kommunikationen kan vælges at være mellem 256 bit til 4096 bit Diffie Hellman, Private Key auth eller Public Key auth.

For yderligere information henvises til Rebex hjemmeside, www.rebex.net, Rebex File Server -> Features -> SSH Server

NOX PCIF (Generel beskyttelse af PC Interface)

Brute force forhindring (Forhindre gentagne forsøg med forkert kode over IP)

I R6 (<9.85x):

IP Interfacet følger de angivne antal forsøg og tid, som er valgt i NOX Config under "Generelt -> Indstillinger -> Bruger -> Betjeningsspærring" ved opnået antal forsøg, spærres IP Interfacet for den pågældende Source IP i det antal minutter der er angivet (standardtid = 3 minutter).

I R7 (>10.0):

SL3: (Bagud kompatibel tilstand med kode alene)

IP Interfacet følger de angivne antal forsøg og tid, som er valgt i NOX Config under "Generelt -> Indstillinger -> Bruger -> Betjeningsspærring" ved opnået antal forsøg, spærres IP Interfacet for den pågældende Source IP i det antal minutter der er angivet (standardtid = 3 minutter).

SL4: (Høj sikkerhed, autentifikation gennem brugernavn og adgangskode, TLS 1.2)

1. Det anbefales at benytte adgangskoder med høj kompleksitet. Kravet til kompleksitet sættes op i NOX Config under "Generelt -> Indstillinger -> Netværksadgang/Netværksnøgle -> Password regler"
2. For hvert forkert loginforsøg sættes der en forsinkelse på 1 ms, dette øges op til 1 sekund, således det vil tage uforholdsmæssigt lang tid at "gætte" koden. Denne forsinkelse fjernes først ved korrekt login.

Kombinationen mellem komplekse koder og forsinkelse betragtes som en særdeles sikker beskyttelse mod Brute force forsøg.

NOX Kode politik (betjeningsenheder på NOX BUS)

Standardkonfigurationen spærrer alle betjeningspaneler i 3 minutter ved 5 forkerte kode indtastninger, efterfølgende spærrer alle paneler i 5 minutter ved indtastning af 6. forkerte indtastning. Det er beskrevet i Forsikring og Pensions (F&P) retningslinjer for AIA anlæg, at det skal være sådan.

I NOX er det programmerbart, så hvis man ønsker en strammere kode politik er det muligt. Vi fraråder at man lemper politikken, da det medfører at anlægget ikke længere lever op til F&P's krav.

NOX Kort + PIN kode politik (CMx interfaces på NOX BUS)

Ved forkert PIN Kode indtastning, er standardopsætningen at der ikke sker noget. Det er en programmerbar funktion, og den er ikke omfattet af regler som ovenstående fra F&P.

I praksis betyder det at hvis man ønsker at et kort spærres efter 3 forkerte PIN indtastninger, er det muligt.

Et spærret kort kan efterfølgende åbnes af en person som kan redigere brugere gennem PC Control.

Dataflow/Båndbredde forbrug

SIMS Server -> SIMS Client

Kommunikationen mellem SIMS Server og SIMS Client består af krypteret data, mest af alt hændelser (tekst), det kræver nærmest ingen båndbredde.

Der er et større behov når man tilslutter en SIMS klient til SIMS Server første gang, da der overføres plantegninger. Disse tegninger caches på klienten, og synkroniseres ved ny forbindelse, såfremt der er sket ændringer.

Hver gang der er en hændelse i NOX Systemet sendes denne til SIMS Serveren, herfra sendes den videre til aktive klienter. Hver hændelse består af max. 1 kB data, en hændelse er en kobling, alarm, bevægelse, osv.

Den anbefalede båndbredde mellem SIMS Server og SIMS Client er 2 Mbit/s, som vil dække langt de fleste tilfælde, da det svarer til 256 hændelser i sekundet. Ved større SIMS installationer med >50 NOX CPU'er kan det være nødvendigt med en højere båndbredde.

NOX CPU -> SIMS Server

Kommunikationen mellem NOX CPU og SIMS Server består af krypteret data, mest af alt hændelser (tekst), det kræver nærmest ingen båndbredde.

Hver gang der er en hændelse i NOX Systemet sendes denne til SIMS Serveren. Hver hændelse består af max. 1 kB data, en hændelse er en kobling, alarm, bevægelse, osv.

Den anbefalede båndbredde mellem NOX CPU og SIMS Server er 0,5 Mbit/s, som vil dække langt de fleste tilfælde, da det svarer til 64 hændelser i sekundet.

NOX CPU -> NOX Config/NOX PC Control

Kommunikationen mellem NOX CPU og NOX Config/NOX PC Control består af krypteret data, mest af alt hændelser (tekst), det kræver nærmest ingen båndbredde.

Hver gang der er en hændelse i NOX Systemet sendes denne til aktive klienter. Hver hændelse består af max. 1 kB data, en hændelse er en kobling, alarm, bevægelse, osv.

Den anbefalede båndbredde mellem NOX CPU og SIMS Server er 0,5 Mbit/s, som vil dække langt de fleste tilfælde, da det svarer til 64 hændelser i sekundet.

Ekstern Applikation -> NOX

Der findes mange typer indgående forbindelsesmuligheder til NOX, fælles for dem er at de typisk er tekstbaserede, derfor kræver de nærmest ingen båndbredde. Nogle af disse muligheder tilbyder også kryptering (SSH/SDK). Da det er variabelt hvad man ønsker at sende til NOX vil det være nødvendigt at lave en vurdering fra sag til sag. Vores erfaring er dog at 2 Mbit/s vil være nok i 99 ud af 100 tilfælde.

NIS2 med NOX og SIMS

EU har skærpet kravene overfor virksomheder og myndigheder på Cyber- og Informationssikkerhedsområdet, samtidig har EU udvidet omfanget af hvilke typer virksomheder der bliver berørt i fremtiden. NIS2 (Network and Information Systems version 2) er rettet mod Elektroniske kommunikationsnetværk, enheder der processerer digitale data, eller systemer der opbevarer data.

NOX

NOX er Certificerede, og godkendte systemer i henhold til EN50131 Klasse 3, højeste sikringsklasse i EU.

I forbindelse med brug af NOX i en virksomhed, er det vigtigt at vide at det udelukkende handler om at sikre kommunikationen med centralenheden, da centralen er den eneste netværksforbundne enhed i et NOX-system. Som det fremgår af dette dokument, er al essentiel netværkskommunikation krypteret, og derfor vil NOX kunne indgå som en sikker enhed i en evt. NIS2 vurdering.

Alle AIA- og ADK-komponenter er forbundet til en RS-485 BUS hvor kommunikationsprotokollen er sikret med en proprietær algoritme, opfundet af NOX Systems.

SIMS

Hvis en virksomhed ønsker at benytte SIMS (Multi Central Management platform til NOX) er samme sag gældende som ovenstående. Det handler udelukkende om at sikre kommunikationen med centralenheden, da centralen er den eneste netværksforbundne enhed i et NOX-system.

SIMS er en Windows baseret applikation, som vil være installeret på en server og kan indgå i kundens patching og vedligeholdelsesplaner på lige fod med virksomhedens øvrige IT-systemer.

Generelle anbefalinger

Det er anbefalet kun at benytte netværksteknologier der understøtter krypteret kommunikation, de enkelte netværksteknologier er beskrevet i detaljer i dette dokument. Vi anbefaler i forbindelse med etablering af ADK at benytte krypteret OSDP-kommunikation til læsere, i kombination med DESFire EV2/EV3 og Secure File læsning som kortteknologi, på denne måde opnås den størst mulige sikkerhed på kort og læser, som samtidig forhindrer kopiering af kort og evt. "man-in-the-middle angreb". Alle NOX AIA og ADK-komponenter der indgår i en Certificeret installation, skal oppebære et sikringsniveau svarende til det af kunden eller evt. 3. part fastsatte niveau og klasse.

Hvis der er behov for yderligere uddybning, eller behov for en uforpligtende snak om sikkerhed på NOX-systemerne, kan man altid kontakte os.

Princip tegning af NOX og SIMS installation i et typisk miljø

