SMLOUVA O DÍLO

Smluvní strany

1. **Státní zdravotní ústav**
   se sídlem Šrobárova 49/48, Vinohrady, 100 00 Praha 10
   IČO: 75010330
   bank. spojení: Česká národní banka
   č. účtu: 1730101/0710
   zastoupená: MUDr. Barborou Mackovou, MHA, ředitelkou
   číslo smlouvy Objednatele: S-SZU/04068/2025

   dále jen „Objednatel“

   Osoba oprávněná jednat ve věcech technických – předmětu smlouvy:

   Osoba oprávněná jednat ve věcech realizace projektu a řízení projektu:

a

2. **BIT SERVIS spol. s r.o.**
   se sídlem: Praha 4, Libušská 144/252, PSČ 14200
   zastoupena: Ondřejem Koutským, jednatelem
   IČO: 45793972
   DIČ: CZ45793972
   bankovní spojení: Česká spořitelna a.s.
   číslo účtu: 1629492/0800

   Zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 11262

   (dále jen „Zhotovitel“)

   Osoba oprávněná jednat ve věcech technických – předmětu smlouvy:

   Osoba oprávněná jednat ve věcech realizace projektu a řízení projektu:

I.
Předmět a účel smlouvy

1. Zhotovitel podal svou nabídku v rámci veřejné zakázky Objednatele s názvem „NÁKUP A IMPLEMENTACE NAC SYSTÉMU v SZÚ“, část A „NAC“ (dále též „**Veřejná zakázka**“), která byla Objednatelem vyhodnocena jako nejvýhodnější. Tato smlouva se tak uzavírá se Zhotovitelem, jako vybraným dodavatelem, za účelem realizace předmětu plnění Veřejné zakázky a v souladu s jeho nabídkou.
2. Zhotovitel se zavazuje pro Objednatele provést na svůj náklad a nebezpečí za podmínek této smlouvy následující dílo:
    a. dodávka, instalace a implementace počítačových programů v rozsahu uvedeném v příloze č. 1,
    b. poskytnutí licence v rozsahu uvedeném v příloze č. 1 a čl. VI. této smlouvy,
    c. konfiguraci systému, testování a školení v rozsahu uvedeném v příloze č. 1,
    d. dodávka a instalace hardware v rozsahu uvedeném v příloze č. 1,

    (dále jen dílo)
3. Objednatel je povinen řádně dokončené dílo převzít a zaplatit Zhotoviteli cenu díla podle čl. III smlouvy.
4. Zhotovitel prohlašuje, že je odborníkem v oblasti předmětu plnění Veřejné zakázky, má dostatečné odborné znalosti, zkušenosti a materiální i personální kapacity nezbytné pro řádné a včasné provedení díla podle této smlouvy. Zhotovitel se zavazuje počínat si tak, aby nedošlo k nedostupnosti jakýchkoli aktivních dat nebo přerušení dostupnosti stávajících systémů Objednatele, kterých se dílo týká.

II.
Doba plnění

1. Dílo je Zhotovitel povinen provést nejpozději do 6 měsíců ode dne účinnosti smlouvy.

III.
Cena a platební podmínky

1. Smluvní strany si sjednávají celkovou cenu díla v částce 1 707 850,00- v Kč bez DPH. Cena díla včetně aktuální sazby DPH činí celkem 2 066 498,50- v Kč.
2. Cena díla bez DPH se sjednává za plnění dle čl. I písmeno a) až d) jako cena pevná a neměnná. Cena díla zahrnuje veškeré náklady Zhotovitele k provedení díla a Zhotovitel není oprávněn žádat úhradu jakýchkoli dalších výdajů.
3. Nárok na zaplacení ceny díla vzniká po předání hotového díla Zhotoviteli na základě oboustranně podepsaného Předávacího protokolu. Cenu díla je Objednatel povinen Zhotoviteli uhradit nejpozději do 30 dnů ode dne doručení řádného daňového dokladu (faktury) na bankovní účet Zhotovitele uvedený v záhlaví. Přechod vlastnictví díla na Objednatele přechází dnem kompletního předání na základě Předávacího protokolu.
4. Objednatel je oprávněn vyúčtovat Zhotoviteli (a Zhotovitel je v takovém případě povinen Objednateli zaplatit) smluvní pokutu ve výši 0,02 % ze smluvené ceny díla za každý den prodlení se splněním závazku Zhotovitele dodat dílo v termínu stanoveném v odst. II. této smlouvy nebo odstranit vady díla podle čl. V odst. 6 smlouvy nebo podle čl. VII. smlouvy.
5. Smluvní strany se dále dohodly na tom, že každá faktura Zhotovitele musí být označena názvem zakázky „NÁKUP A IMPLEMENTACE NAC SYSTÉMU v SZÚ“, část A „NAC“, reg. č. projektu a názvem projektu „Kybernetická bezpečnost ve Státním zdravotním ústavu, registrační číslo CZ,06,01/00/22_005/0002815; Evidenční číslo dotace 135V151000013“) “.

6. Zhotovitel není oprávněn požadovat poskytnutí jakékoli zálohy nebo přiměřené části ceny díla před dokončením díla.
7. Zhotovitel přebírá nebezpečí změny okolností ve smyslu § 2620 odst. 2 občanského zákoníku.

IV.

Povinnosti smluvních stran

1. Zhotovitel je povinen dílo provést samostatně, v souladu s právními předpisy a odbornými standardy a je povinen dbát na oprávněné zájmy Objednatele. Zhotovitel je povinen upozornit Objednatele na nevhodnou povahu věcí převzatých od Objednatele k provedení díla či nevhodnost jeho pokynů (zejm. požadavků na konfiguraci díla), jestliže Zhotovitel mohl tuto nevhodnost při vynaložení odborné péče zjistit.
2. Zhotovitel je povinen dílo provést pod svým osobním vedením a na provádění díla se musí podílet realizační tým, jehož členové byli uvedeni v nabídce Zhotovitele v rámci zadávacího řízení Veřejné zakázky a jsou uvedeni v Příloze č. 2 – Realizační tým. Případná změna těchto členů realizačního týmu podléhá schválení Objednatele.
3. Zhotovitel je povinen dílo provést v sídle Objednatele na adrese uvedené v záhlaví této smlouvy. Je-li to možné a účelné, je Zhotovitel oprávněn provádět činnosti nutné k provedení díla ze svého sídla (např. přímý vzdálený přístup do informačního systému Objednatele, instalace technologií, apod.).
4. Objednatel je povinen poskytnout Zhotoviteli veškerou potřebnou součinnost nutnou k provedení díla. Takto je Objednatel zejména povinen sdělit Zhotoviteli informace a předat Zhotoviteli dokumenty nezbytně nutné k provedení díla, umožnit Zhotoviteli přístup do prostor Objednatele, v nichž je dílo prováděno apod.
5. Ocitne-li se Objednatel přes písemné upozornění Zhotovitele v prodlení se splněním povinnosti poskytnout Zhotoviteli součinnost dle předchozí věty, prodlužuje se o dobu prodlení doba ke zhotovení díla.
6. Zhotovitel je povinen uchovávat po dobu 10 let od ukončení realizace díla doklady související s realizací díla a umožnit osobám objednatele oprávněným k výkonu kontroly provést kontrolu těchto dokladů. Lhůta dle předcházející věty začíná běžet od 1. ledna následujícího kalendářního roku po předání díla.
7. Zhotovitel je povinen po celou dobu trvání smlouvy udržet v platnosti pojištění odpovědnosti za újmu způsobenou při své podnikatelské činnosti s pojistným krytím minimálně ve výši 4.000.000 Kč za každou pojistnou událost.
8. Objednatel je oprávněn vyúčtovat Zhotoviteli (a Zhotovitel je v takovém případě povinen Objednateli zaplatit) smluvní pokutu ve výši 50.000 Kč vč. DPH za každé jednotlivé porušení povinností podle tohoto článku smlouvy.

V.

Předání díla

1. Dílo je provedeno jeho dokončením a předáním Objednateli, anebo okamžikem, kdy se Objednatel ocitl v prodlení s převzetím dokončeného díla.
2. Po dokončení díla Zhotovitel vyzve Objednatele k převzetí díla a poskytne mu veškerý přístup pro testování díla v délce alespoň třech (3) pracovních dnů, ve kterém Objednatel posoudí, zda je dílo způsobilé převzetí a splňuje podmínky této smlouvy.
3. O předání a převzetí díla jsou smluvní strany povinny mezi sebou sepsat předávací protokol.

4. Objednatel může dílo převzít i v případě, že dílo vykazuje drobné vady a nedodělky, které nemají vliv na celkovou funkčnost díla. Vykazuje-li dílo vady, které brání jeho řádnému užívání, Objednatel dílo nepřevezme a sdělí písemně Zhotoviteli své odůvodnění.
5. Smluvní strany vylučují možnost převzetí díla po částech.
6. Zhotovitel je povinen odstranit vady nebo nedodělky díla uvedené v předávacím protokolu bez zbytečného odkladu, nejpozději do 10 dnů. Pro posouzení odstranění vad se uplatní postup předání díla podle tohoto odstavce obdobně. Náklady na odstranění vad nebo nedodělků nese Zhotovitel.

VI.
Duševní vlastnictví

1. Uživatelská práva poskytnutá Objednateli jsou nevýhradní a nepřenosná na třetí osoby, Objednatel není v žádném případě oprávněn šířit právo užívání aplikačního programového vybavení na třetí osoby. Uživatelská práva nejsou časově omezena, aplikační programové vybavení může být užíváno pouze v sídle Objednatele.

2. Zhotovitel je dále povinen v rámci plnění díla zajistit poskytnutí Objednateli nezbytných časově neomezených licencí k autorským dílům třetích stran (např. operační systémy pro pracovní stanice, ovladače a další software). Cena za poskytnutí těchto licencí je součástí ceny díla a poskytovaná licence se řídí licenčními podmínkami daného poskytovatele software.

3. Zhotovitel se zavazuje zajistit, aby na dílu nebo jakékoli jeho části nevázla jakákoli práva třetích osob. Prohlašuje zejména výslovně, že vypořádal veškeré závazky vůči všem případným autorům a žádný z těchto autorů nemá nárok na jakoukoliv dodatečnou odměnu v souvislosti s dílem nebo jeho částí. Ukáží-li se tato prohlášení jako nepravdivá, může Objednatel dle svého uvážení požadovat po Zhotoviteli i to, aby veškeré závazky na svůj náklad vypořádal, případně aby nahradil dotčenou část díla jiným řešením.

VII.
Záruka

1. Zhotovitel Objednateli poskytuje záruku za jakost díla po dobu min. 36 měsíců na HW a min. 12 měsíců na SW (pokud není v příloze č. 1 uvedeno jinak) ode dne předání do provozu. Náklady na odstranění vad krytých zárukou za jakost nese Zhotovitel.
2. Záruka na jakost se nevztahuje na vady způsobené vyšší mocí a vady způsobené neodbornou obsluhou, protiprávním jednáním třetí osoby či Objednatele a elektrickou napájecí sítí a komunikační infrastrukturou Objednatele.
3. Nároky ze záruky je Objednatel povinen vůči Zhotoviteli uplatnit písemně u oprávněné osoby ve věcech technických uvedené v záhlaví této smlouvy („**Incident**“).
4. Požadavek na řešení Incidentu musí obsahovat popis Incidentu, zejm. toho, jak a v jakých situacích se Incident projevuje. Zhotovitel provede předběžné posouzení Incidentu a odešle Objednateli prvotní reakci na jeho požadavek, v níž informuje Objednatele o okolnostech podstatných pro řešení Incidentu a zahájí práci na odstranění vady („**Reakční doba**“).
5. Zhotovitel odstraní příčinu vzniku Incidentu nebo jinak obnoví funkčnost díla („**Doba pro řešení**“).
6. Délka Reakční doby a Doby pro řešení závisí na následující kategorizaci Incidentů:

Název kategorie	Reakční doba	Doba pro řešení
Kategorie A	24 hodin	48 hodin
Kategorie B	48 hodin	5 pracovních dní
Kategorie C	5 pracovních dnů	podle dohody

Incidenty spadají do kategorií dle následujícího klíče:

i. **Kategorie A**: Dílo není použitelné ve svých základních a klíčových funkcích, což znemožňuje jeho užívání všem nebo většině jeho uživatelů a ohrožuje běžný provoz Objednatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné škody.

ii. **Kategorie B**: Funkčnost díla je omezena tak, že tento stav omezuje běžné užívání díla.

iii. **Kategorie C**: Veškeré vady, které nespadají do Kategorie A a Kategorie B, tedy drobné závady neznemožňující ani neomezující základní funkčnost a běžné užívání díla.

VIII.
Důvěrnost informací

1. Smluvní strany jsou povinny zachovávat mlčenlivost o všech skutečnostech, o kterých se o sobě navzájem dověděly při realizaci této smlouvy, a které jsou neveřejné a hospodářsky využitelné, anebo mají povahu obchodního tajemství.
2. Povinnost zachovávat mlčenlivost dle tohoto článku smlouvy znamená zejména povinnost zdržet se jakéhokoli jednání, kterým by důvěrné informace byly jakoukoliv formou sděleny nebo zpřístupněny třetí osobě nebo by byly důvěrné informace využity v rozporu s jejich účelem pro vlastní potřeby nebo potřeby třetí osoby anebo by bylo umožněno třetí osobě jakékoliv využití těchto Důvěrných informací.
3. V případě, že Zhotovitel bude mít přístup k osobním údajům zpracovávaným Objednatelem, smluvní strany se zavazují bezodkladně uzavřít smlouvu o zpracování osobních údajů splňující požadavky právních předpisů.

4. Objednatel je oprávněn vyúčtovat Zhotoviteli (a Zhotovitel je v takovém případě povinen Objednateli zaplatit) smluvní pokutu ve výši 50.000 Kč vč. DPH za každé jednotlivé porušení povinností podle tohoto článku smlouvy.

IX.
Platnost smlouvy

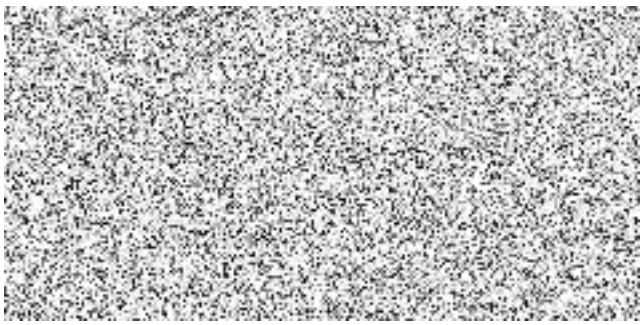
1. Smlouva může být měněna pouze písemně. Práva a povinnosti touto smlouvou neupravené se řídí příslušnými právními předpisy České republiky, zejména občanským zákoníkem.
2. Tato Smlouva je uzavřena elektronickou formou s využitím kvalifikovaných elektronických podpisů osob oprávněných právně jednat v zastoupení Smluvních stran.
3. Tato smlouva je uzavřena na dobu určitou do doby provedení díla a nabývá platnosti ke dni jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
4. Nedílnou součást této smlouvy tvoří Příloha č. 1 – Podrobná specifikace díla a Příloha č. 2 – Realizační tým.

X.
Závěrečná ustanovení

1. Smluvní strany shodně prohlašují, že tato smlouva odpovídá jejich skutečné, vážné a svobodné vůli, a že se seznámily a souhlasí s jejím obsahem, což potvrzují svými podpisy smlouvy.
2. Zhotovitel se za podmínek stanovených touto Smlouvou zavazuje jako osoba povinná dle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, spolupůsobit při výkonu finanční kontroly, mj. umožnit všem subjektům oprávněným k výkonu kontroly Projektu, zejména Řídicímu orgánu OP IROP, přístup ke všem dokumentům, tedy i k těm částem nabídek, smluv a souvisejících dokumentů, které podléhají ochraně podle zvláštních právních předpisů (např. obchodní tajemství), a to za předpokladu, že budou splněny požadavky kladené právními předpisy; tuto povinnost rovněž zajistí Zhotovitel u případných poddodavatelů Zhotovitele.

V Praze dne dle data el. podpisu

V Praze dne dle data el. podpisu



Příloha č. 1 – Podrobná specifikace díla

Technické požadavky

Obecný popis systému

NAC je pokročilý systém pro správu síťové bezpečnosti, který poskytuje komplexní kontrolu a ochranu vaší síťové infrastruktury. Tento nástroj je navržen tak, aby zajišťoval bezpečnost všech zařízení připojených k síti, ať už se jedná o zařízení zaměstnanců, hostů nebo IoT zařízení. NAC nabízí robustní ochranu proti kybernetickým hrozbám a zajišťuje, že pouze autorizovaná zařízení a uživatelé mají přístup k síťovým zdrojům.

Funkce

1. Visibility (Viditelnost)

NAC poskytuje detailní přehled o všech zařízeních připojených k síti. Díky pokročilým možnostem skenování a monitorování můžete snadno identifikovat a sledovat všechna zařízení, která se připojují k vaší síti, včetně těch, která jsou připojena přes VPN nebo WiFi. Systém automaticky detekuje nové zařízení a poskytuje detailní informace o jeho typu, stavu a aktivitách. Tato viditelnost je klíčová pro efektivní správu a ochranu sítě.

2. (Endpoint Profiling) Profilování koncových zařízení

Profilování je jednou z klíčových funkcí systému NAC, která umožňuje detailní identifikaci a klasifikaci všech zařízení připojených k síti. NAC využívá pokročilé techniky skenování a analýzy, aby automaticky rozpoznal typ zařízení, jeho operační systém, výrobce, model a další charakteristiky. Tento proces probíhá v reálném čase a poskytuje administrátorům přesný a aktuální přehled o všech zařízeních v síti. Díky profilování může NAC efektivně aplikovat bezpečnostní politiky na základě konkrétních atributů zařízení, čímž zajišťuje, že každé zařízení obdrží odpovídající úroveň přístupu a ochrany. Profilování také umožňuje rychlou detekci neznámých nebo podezřelých zařízení, což je klíčové pro prevenci a reakci na potenciální bezpečnostní hrozby.

2. Control (Kontrola)

NAC umožňuje administrátorům nastavit a aplikovat bezpečnostní politiky pro všechna zařízení připojená k síti. Můžete definovat, kdo a co může přistupovat k různým částem vaší sítě, a zajistit, že pouze autorizovaná zařízení mají přístup k citlivým datům. Systém podporuje dynamické politiky, které se automaticky přizpůsobují změnám v síťovém prostředí. To zajišťuje, že vaše síť zůstane bezpečná i v případě, že se připojí nové nebo neznámé zařízení.

3. Response (Reakce)

NAC je vybaven schopností rychle reagovat na bezpečnostní incidenty. V případě detekce podezřelé aktivity nebo porušení bezpečnostních politik může systém automaticky izolovat postižené zařízení, čímž zabrání šíření hrozby. NAC také poskytuje nástroje pro detailní analýzu incidentů a podporuje integraci s dalšími bezpečnostními systémy, což umožňuje koordinovanou a efektivní reakci na kybernetické útoky.

Nasazení na celou přístupovou síť, VPN i WiFi

NAC je navržen pro snadnou integraci do různých typů síťových prostředí. Podporuje nasazení na celou přístupovou síť, včetně VPN a WiFi, což zajišťuje jednotnou a konzistentní úroveň bezpečnosti napříč všemi přístupovými body. Systém je kompatibilní s širokou škálou síťových zařízení a infrastruktury od různých výrobců, což usnadňuje jeho implementaci do stávajících síťových prostředí. Díky tomu můžete snadno rozšířit bezpečnostní politiky na všechny části vaší sítě a zajistit, že každé zařízení je chráněno bez ohledu na to, odkud se připojuje.
NAC je ideálním řešením pro organizace, které hledají efektivní způsob, jak spravovat a chránit svou síťovou infrastrukturu před stále sofistikovanějšími kybernetickými hrozbami. S jeho pomocí můžete zajistit, že vaše síť bude bezpečná, spolehlivá a připravená na budoucí výzvy.

Požadavek na funkcionalitu	Splňuje ano/ne
OBECNÉ POŽADAVKY NA PLATFORMU	
Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM (HW alternativa není poptávána)	ANO
Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance	ANO
Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami	ANO
Autentizační brány musí být nasazené mimo samotný datový tok (tzv. inline řešení není akceptovatelné)	ANO
Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem	ANO
Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky	ANO
Schopnost NAC řešení komunikovat se síťovými prvky, drátovými i bezdrátovými, jiných výrobců pomocí SNMP a CLI a vymáhat na nich definované bezpečnostní politiky bez nutnosti využití 802.1x nebo MAB	ANO
Možnost instalace samostatného NAC řešení v podobě pouze enforcement brány bez nutnosti nákupu dalších prvků, jako například centrální management. Pokud je další prvek nutný, musí být součástí nabídky.	ANO
Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě	ANO
Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting	ANO
Všechny požadované funkce pokrývá jeden typ licence a je možné dodatečně zvýšit počet licencí v systému	ANO
Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů	ANO
POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ	
Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN)	ANO
Možnost detailní profilace připojeného zařízení a klienta a to buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem	ANO

sítě nebo komunikací s externím systémy a to bez nutnosti dodatečného licencování této funkcionality	
Podpora politik pro automatickou profilaci zařízení (minimálně na základě: SNMP, RADIUS, SYSLOG, DHCP, API, SSH, NMAP, DHCP fingerprinting, HTTP(s), IP range, telnet, expect scripty, vyhodnocení TCP/UDP portů, VENDOR OUI/MAC, WMI profil, pollování firewallu a vyhodnocování síťové komunikace, perl skripty) a to bez nutnosti dodatečného licencování této funkcionality	ANO
Periodická kontrola připojeného zařízení, zda odpovídá profilu, na základě kterého bylo zařízeno vpuštěno do sítě a možnost odpojit zařízení v případě, kdy nesplňuje podmínky původního profilu	ANO
Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS	ANO
Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí standardních Radius atributů	ANO
Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL	ANO
Podpora 802.1x	ANO
Podpora MAB autentizace	ANO
Podpora tvorby lokálních účtů a lokální autentizace	ANO
Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě	ANO
Podpora funkce RADIUS proxy	ANO
Možnost integrace se stávající CA (certifikační autorita)	ANO
Podpora agentů pro operační systémy: Windows, MacOS, Linux (agent dodává detailní informace o počítači, informace o login/logout, umožňuji spouštění skriptů a zajišťuje notifikace pro uživatele) a licence pro tyto agenty je součástí dodané licence	ANO
Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP	ANO
Podpora captive portál v rámci autentizační brány s plně editovatelným prostředí	ANO
Minimálně 5 různých captive portálů	ANO
Podpora tzv. sponzorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email	ANO
NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovní přístupové vrstvy v případě zjištění bezpečnostního incidentu	ANO
Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty	ANO
Podpora integrace s poptávaným NGFW a analytickým nástrojem nad provozem poptávaného NGFW	ANO
Podpora alespoň RSSO komunikace s NGFW	ANO

Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele	ANO
POŽADAVKY NA ENDPOINT COMPLIANCE	
Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici	ANO
Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě)	ANO
Kontrola stavu AV na stanici	ANO
Kontrola stavu registrů	ANO
Kontrola existence konkrétních souborů v lokálním filesystému	ANO
Ověření domény	ANO
Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name,	ANO
Ověření verze a patch levelu operačního systému	ANO
Podpora sběru informací o instalovaných aplikacích na endpointech	ANO
Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál	ANO
Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance	ANO
AUTOMATIZACE	
Možnost definovat playbook, nativně v GUI, který bude vykonávat automatické akce na základě definované události a následné akce dle aktuálního stavu (minimálně v podobě blokace portu, změny L2 segmentu, aplikace skriptu)	ANO
Řešení je možné obsluhovat pomocí výrobcem popsaných API volání	ANO
Možnost automatické tvorby tiketů v systému ServiceNow na základě definované události	ANO
REPORTING	
Možnost tvorby reportů o stavu platformy a stavu připojených zařízení v reálném čase a alespoň zpětně o jeden týden. Reporting je nativní funkce dostupná v GUI bez nutnosti dodatečného licencování	ANO
NOTIFIKACE ADMINISTRÁTORŮ A UŽIVATELŮ	
Možnost napojení autentizační brány na SMS nebo email bránu promocí konektoru přímo z GUI	ANO
POŽADAVKY NA LICENCE A PODPORU VÝROBCE	
Licence pro min. 1500 endpointů	ANO
Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO
Centrální autentizační server s podporou 2FA - obecné požadavky na platformu	
VM appliance pro virtualizační platformu zadavatele (VMWARE ESX, Microsoft Hyper-V, KVM)	ANO
management identit, plnohodnotná AAA funkcionalita, integrované funkce AAA pro připojení z VPN	ANO
Požadujeme systém v režimu vysoké dostupnosti s podporou A-P nebo A-A clusteru	ANO
Podpora nabízených funkcí pro minimálně 1000 uživatelů	ANO

Licenčně rozšířitelné	ANO
Možnost automaticky synchronizovat uživatele z Active Directory	ANO
Možnost vytvářet lokální uživatele a skupiny	ANO
Podpora 2FA pomocí tokenů (aplikace pro iOS a Android, HW token)	ANO
Možnost přidání min. 20 tokenů s možností rozšíření	ANO
Podpora 2FA pomocí SMS a emailu	ANO
Podpora ověřováni ze sociálních sítí (např.: facebook, linkedin)	ANO
Možnost definovat zařízení na základě MAC adresy	ANO
Funkce LDAP/LDAPS serveru	ANO
Možnost automatického importu identit ze vzdálených LDAP serverů	ANO
Funkce TACACS+ serveru	ANO
Funkce Radius serveru	ANO
Podpora radius accounting v proxy režimu	ANO
Funkce SAML 2.0 IdP, IdP proxy	ANO
Možnost napojení a ověřování z externího Radius, LDAP SAML a OAuth server	ANO
Podpora SSO autentizace uživatelů v prostředí domény MS Windows	ANO
Podpora Kerberos	ANO
podpora EAP metod EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-GTC	ANO
Funkce certifikační autority	ANO
Možnost přidání min. 3000 uživatelských certifikátů	ANO
Podpora SCEP a CRL	ANO
Podpora captive portálu	ANO
Podpora samoobslužných portálů (reset hesla, editace uživatelských údajů, přidělení tokenů)	ANO
Podpora 2FA pro Outlook Web Access pomocí nativního klienta	ANO
Podpora mechanismu 2FA pro koncové stanice a přihlášení do systému Windows	ANO
Podpora FIDO2 ověření	ANO
Podpora push notifikací pro 2FA a mobilní aplikaci	ANO
Podpora REST API (pokud tato funkce vyžaduje licenci, tak musí být součástí dodávky)	ANO
Podpora active-pasive HA	ANO
Podpora Config sync HA	ANO

Ostatní podmínky:

- Na základě výsledků analýzy zvážil Zadavatel prostředí nasazení, rizika, stávající opatření a též možná nová bezpečností opatření ke snížení vysoké hodnoty rizika a dospěl k závěru, že jediným bezpečnostním opatřením, kterým je objektivně možné snížit hodnotu rizika na akceptovatelnou úroveň technických a programových prostředků společností před kterými NÚKIB varoval oproti jiným, je úplné vyloučení prostředků dotčených společností z této zakázky.
- Exaktně se jedná o vyloučení „použití technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation“.

Věcná část nabídky. Vlastní technický popis konkrétního nabízeného plnění, které musí odpovídat technické specifikaci

Představení výrobce FORTINET

Společnost Fortinet založil v roce 2000 Ken Xie, vizionář a dřívější prezident a CEO společnosti NetScreen. Prvním cílem společnosti Fortinet byl vývoj konsolidovaných bezpečnostních zařízení s vysokým stupněm vzájemné integrace navržených do segmentu operátorů. Od počátku byl kladen důraz na vysoký výkon nabízených appliance, jehož bylo dosahováno pomocí vlastního vývoje specializovaných integrovaných obvodů (čipů) pro hardwarovou akceleraci. Díky unikátní koncepci dosahuje každý produkt společnosti Fortinet v zákaznickém prostředí vysokého výkonu, a to při zachování přívětivé cenové politiky.

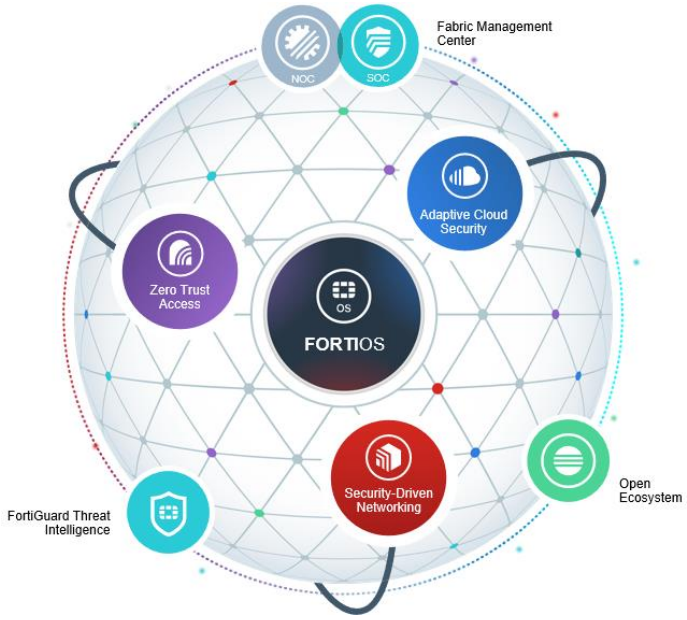
Vysoká účinnost ochrany proti síťovým hrozbám je zajištěna také vlastní „threat“ laboratoří, kterou společnost Fortinet provozuje pod názvem FortiGuard. Pracovníci této laboratoře nepřetržitě monitorují a vyhodnocují aktuální dění a hrozby v síti internet a podle zachycených skutečností aktualizují jednotlivé databáze a enginy, které se následně distribuují ke koncovým zákaznickým zařízením. Společnost Fortinet klade velký důraz rovněž na vlastní vývoj operačního systému pro svá zařízení (FortiOS). Operační systém je koncipován přesně na míru jednotlivým zařízením a plně využívá možnosti hardware akcelerace.

Unikátní koncepce (tedy šíře produktového portfolia, velké množství konsolidovaných bezpečnostních funkcí, vlastní vývoj hardware, vlastní vývoj operačního systému – software, vlastní „threat“ laboratoř FortiGuard) nabízí zákazníkovi dosažení nejvyšší možné úrovně zabezpečení sítě a souvisejících komponent, které se soustředí na end-to-end zabezpečení následujících oblastí:

- Síťová bezpečnost (HW i VM appliance)
- Zabezpečení datacenter
- Zabezpečení cloudových služeb
- Zabezpečení přístupové vrstvy LAN a WAN
- Zabezpečení infrastruktury (switching a routing)
- Zabezpečení přenášeného obsahu (content security, L7 security)
- Ochrana a zabezpečení koncového zařízení (endpoint security)
- Granulární zabezpečení jednotlivých aplikací (aplikační firewally)

Klíčové výhody technologie FORTINET

V produktovém portfoliu společnosti Fortinet jsou desítky produktových řad zaměřených na end-to-end bezpečnost začínající od zabezpečení samotného koncového zařízení, přes přístupovou vrstvu (síťové přepínače a bezdrátové přístupové body), centrální firewall prvky (interní segmentační firewally), nástroje pro aplikační bezpečnost (aplikační firewally, nástroje pro ochranu před DDoS útoky), nástroje pro doručení aplikace (ADC), nástroje pro autentizaci uživatelů (centrální autentizační appliance), nástroje pro ochranu před pokročilými druhy hrozeb (sandboxing) a samozřejmě nástroje pro korelaci bezpečnostních incidentů (SIEM), ukládání logů, reporting a centrální správu.



Myšlenka Fortinet Security Fabric vychází z toho, že pokud každý z výše uvedených produktů nahlíží na bezpečnost ze svého úhlu pohledu, pak nemusí být schopen pozorovat dění v síti s globálním nadhledem. Proto společnost Fortinet přichází s unikátní platformou (Fortinet Security Fabric), která zajišťuje interoperabilitu mezi jednotlivými produktovými řadami, čímž umožňuje rychlé šíření informací o odhalených hrozbách napříč instalovanou bází bezpečnostních produktů, a dále pak lépe a názorněji vizualizuje posbírané informace a nabízí funkci automatizace zásahu v okamžiku detekce incidentu.

Účast ve Fortinet Security Fabric není omezená pouze na produkty značky Fortinet, ale přes otevřené API máme již dnes řadu technologických partnerů, kteří se dokážou integrovat s funkcemi Fortinet Security Fabric. Mezi hlavní značky patří např.: McAfee, Carbon Black, Sentinel One, Symantec, Ziften, Amazon Web Services, Oracle, VMWare, Cisco, Openstack, Brocade, HP, Qualys, IBM Security, WhiteHat, Splunk, Adva, Ribbon, Verisgn, Intel, Braeadfor Networks, Nozomi Networks, Pulse Secure, Cyberark a řada dalších.

Popis technologie FortiNAC

FortiNAC je řešení společnosti Fortinet určené k řízení přístupu do sítě, které rozšiřuje možnosti bezpečnostní architektury Security Fabric. FortiNAC poskytuje ochranu proti IoT hrozbám, rozšiřuje kontrolu i na zařízení jiných výrobců, a koordinuje automatické reakce na široké spektrum síťových událostí.

FortiNAC poskytuje ucelený přehled a podrobný profily zařízení připojených k síti včetně přenosných. Využívá k tomu různé zdroje informací o zařízeních a jejich chování.

FortiNAC dokáže implementovat segmentační pravidla a měnit konfiguraci u přepínačů a bezdrátových zařízení od více než 70 výrobců. Rozšiřuje dosah bezpečnostní architektury Security Fabric v heterogenních prostředích.

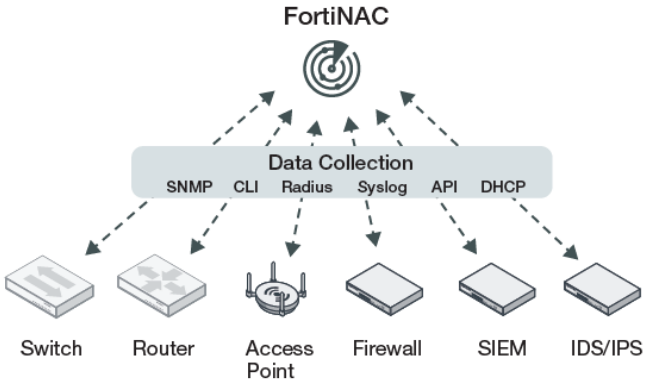
FortiNAC umožňuje reagovat na události v síti v řádu jednotek sekund a neutralizovat hrozby dříve, než se stačí rozšířit. Nabízí rozsáhlý soubor přizpůsobitelných automatizačních pravidel, která dokáží okamžitě vyvolat změny v konfiguraci, je-li zaznamenáno sledované chování.

Hlavní charakteristiky

- Skenování sítě bez agenta kvůli detekci a klasifikaci zařízení
- Soupis veškerých zařízení v síti
- Předávání informací o událostech do SIEM s podrobnými kontextovými daty zkracuje dobu nutnou k vyšetřování
- Vyhodnocení rizik u každého koncového bodu připojeného k síti
- Automatizace procesu připojení velkého počtu koncových bodů, uživatelů a hostů
- Vynucení dynamického řízení přístupu k síti a možnost její segmentace
- Zkrácení dobu neutralizace hrozby z dnů na sekundy
- Sada předpřipravených šablon pro reporting, compliance a analýzu

Přehled o připojených zařízeních

Pro zabezpečení proměnlivé sítě je zásadní znalost její struktury. FortiNAC prohledává síť a bez pomoci softwarového agenta detekuje všechny uživatele, aplikace a zařízení. Využívá až 13 různých technik k sestavení profilu každého prvku na základě pozorovaných charakteristik a chování. Zaznamenává také potřebu aktualizací softwaru kvůli opravě bezpečnostních chyb. FortiNAC rovněž identifikuje uživatele a uplatňuje patřičná přístupová pravidla nastavená podle rolí na ochranu důležitých a citlivých dat a zajišťuje soulad s interními, oborovými a legislativními předpisy.



Dynamické řízení sítě

Jakmile jsou zařízení a uživatelé identifikováni, umožňuje FortiNAC podrobně segmentovat síť tak, aby zařízení a uživatelé měli přístup k potřebným zdrojům, a zároveň blokuje nerelevantní části sítě. FortiNAC využívá dynamické řízení přístupu k síti podle rolí. Seskupováním podobných aplikací a dat vytváří logické segmenty, k nimž povoluje přístup jen určitým

skupinám uživatelů. Je-li některé zařízení napadeno, má útočník pouze omezenou možnost pohybu v síti.

Zajištění integrity zařízení před jejich připojením k síti minimalizuje rizika a možné šíření škodlivého softwaru. FortiNAC ověřuje konfiguraci zařízení již při pokusu o připojení k síti. V případě, že konfigurace neodpovídá požadavkům, zachází se se zařízením patřičným způsobem – je například vyčleněno do izolované nebo omezené podsítě VLAN.

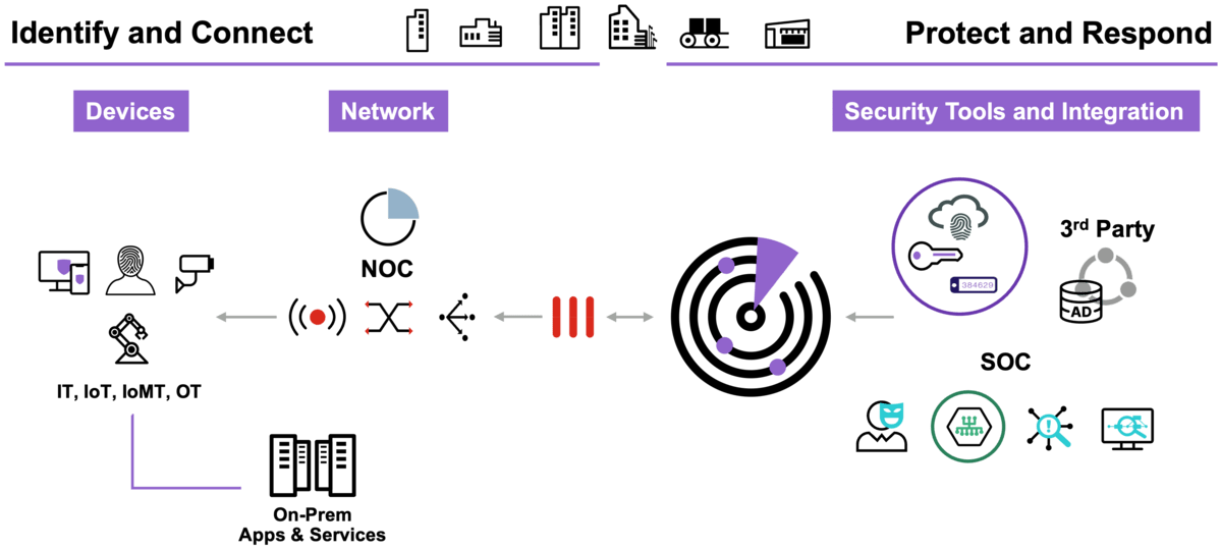
FortiNAC síť nepřetržitě sleduje a může přidělenou úroveň přístupu následně přizpůsobovat podle změn chování zařízení.

Okamžitá automatizovaná reakce

Je-li identifikováno napadené nebo zranitelné zařízení, FortiNAC ihned iniciuje automatizovanou reakci na ochranu před nebezpečím. Ta může spočívat v ukončení připojení, omezení přístupu k síti, izolaci v karanténní podsíti VLAN a různých typech upozornění. Automatizace celého procesu fakticky stírá rozdíl mezi bezpečnostním operačním centrem (SOC) a síťovým operačním centrem (NOC) a zkracuje dobu nutnou k potlačení hrozby ze dnů na sekundy.

Vysoká dostupnost

FortiNAC nabízí vysokou dostupnost pro obnovu po havárii, aby byla zajištěna redundance. Tohoto stavu je dosaženo prostřednictvím aktivních a pasivních instancí, kdy se pasivní (záložní) stane aktivním, když hlavní síť již nefunguje normálně. FortiNAC Manager může podle potřeby spravovat několik vysoce dostupných clusterů distribuovaných po síti.



Produktový list FortiNAC – aktivní odkaz

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf

Popis technologie FortiAuthenticator

Jedná se o centralizované řešení pro správu a ochranu identit uživatelů v síti. Poskytuje širokou škálu funkcí zaměřených na autentizaci, autorizaci a správu uživatelských identit.

Hlavní funkce:

- Centrální autentizace a správa: umožňuje centrální správu uživatelských identit a autentizačních metod. Tímto způsobem lze snadno spravovat přístupová práva a autentizovat uživatele napříč různými systémy a službami.
- 2FA autentizace: zvyšuje zabezpečení přihlašování tím, že vyžaduje nejen uživatelské jméno a heslo, ale také druhý autentizační faktor, například token nebo mobilní aplikaci.
- Integrované správa certifikátů: může sloužit jako certifikační autorita (CA) pro vydávání a správu digitálních certifikátů. To umožňuje použití certifikátů pro ověřování uživatelů a zabezpečení komunikace.
- Synchronizace uživatelských účtů: umožňuje synchronizaci uživatelských účtů s různými externími databázemi, jako jsou Active Directory nebo LDAP. Tím se snižuje nutnost manuální správy uživatelských účtů a zvyšuje se přesnost dat.
- Integrace s dalšími produkty Fortinet: FortiAuthenticator je navržen tak, aby se snadno integroval s dalšími produkty společnosti Fortinet, jako je například řada firewalů FortiGate nebo VPN řešení FortiClient. Tímto způsobem může poskytnout pokročilou autentizaci a správu uživatelských identit pro celou síťovou infrastrukturu
- Podpora IEEE802.1X pro LAN a wireless
- FIDO2: známý také jako bezheslový ověřování. FIDO2 je technika umožňující použití silného jednofaktorového (bez hesla), dvoufaktorového a vícefaktorového ověřování pro zvýšení ochrany

Metody Single Sign-On:

- Active Directory Polling – ověřování uživatelů do adresáře Active Directory se zjišťuje pravidelným dotazováním řadičů domény. Při zjištění přihlášení uživatele se uživatelské jméno, IP adresa a údaje o skupině zadají do databáze správy identit uživatelů zařízení FortiAuthenticator a podle místních zásad mohou být sdíleny s více zařízeními FortiGate
- FortiAuthenticator SSO Mobility Agent – pro složité architektury domén, kde není možné nebo žádoucí dotazování řadičů domény, je alternativou klient SSO FortiAuthenticator. Klient, který je distribuován jako součást produktu FortiClient nebo jako samostatná instalace pro počítače se systémem Windows, posílá události přihlášení, změny IP stack a odhlášení do serveru FortiAuthenticator, čímž odstraňuje potřebu metod dotazování.
- FortiAuthenticator and Wifgets – pro systémy, které nepodporují dotazování AD nebo kde klient není proveditelný, poskytuje FortiAuthenticator autentizační portál. Tento portál umožňuje uživatelům ruční autentizaci do FortiAuthenticatoru a následně do sítě. Aby se minimalizoval dopad opakovaných přihlášení vyžadovaných pro ruční ověřování, je k dispozici sada widgetů pro vložení do intranetu organizace, které automaticky přihlašují uživatele pomocí souborů cookie prohlížeče, kdykoli vstoupí na domovskou stránku intranetu.

Produktový list FortiAuthenticator – aktivní odkaz

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf

Sizing řešení FortiNAC/FortiAuthentificator

Kód produktu	Popis produktu	Počet
FC5-10-FNAC1-213-01-60	FortiNAC Subscription PLUS License for 100 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.	5
FC6-10-FNAC1-213-01-60	FortiNAC Subscription PLUS License for 1.000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.	1
FTM-ELIC-10	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10 users. Electronic license certificate. License transfer between devices is not allowed.	2
FAC-VM-BASE	VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms	1
FAC-VM-1000-UG	FortiAuthenticator-VM 1000 users license upgrade	1
FC2-10-0ACVM-248-02-60	FortiCare Premium Support (1 - 1100 USERS)	1

Instalace a implementace

Instalace virtuální appliance v režimu vysoké dostupnosti (Active-Passive)
Základní konfigurace (IP, přístupy, atd...) a registrace licencí
FortiNAC konfigurace dle zadání (MS AD, izolace, Certifikáty pro NAC)
Napojení na výrobcem podporované aktivní prvky (max. 30)
Persistent Agent - distribuce na koncová zařízení (max. 10)
Konfigurace vzorových politik pro přístup do sítě (max. 5)
Konfigurace vzorových profilerů pro kategorizaci zařízení (max. 3)
Konfigurace vzorových compliance politik (max. 3)
Schůzky pro zadání a požadavky objednatele, konzultace řešení

Instalace virtuální appliance
Základní konfigurace (IP, přístupy, atd...) a registrace licencí
Napojení na zdroj identit (Radius, LDAP,..), max. 2
Vytvoření jedné ověřovací metody, např. Radius
Import tokenů pro MFA
Vytvoření vzorových politik pro ověření uživatele/zařízení (max. 10)
Schůzky pro zadání a požadavky objednatele, konzultace řešení

Školení FortiNAC a FortiAuthenticatoru (vzdálená forma)
Dokumentace FortiNAC a FortiAuthenticatoru

Příloha č. 2 – Realizační tým