PŘÍLOHA Č. 1 – SPECIFIKACE PŘEDMĚTU PLNĚNÍ

Předmětem plnění je rozšíření systému „Centrální správy a monitoringu IP adresního prostoru“ (dále jen CSMIP) spočívající v dodávce, implementaci, uvedení do provozu záložní lokality Datového centra DC2 kupujícího na adrese Jílovská 1148/14, Praha 4, včetně servisní podpory na 3 roky a údržby stávajícího systému CSMIP na 3 roky.

ZJEDNODUŠENÝ POPIS STÁVAJÍCÍHO NÁSTROJE CSMIP KUPUJÍCÍHO

Nástroj zajištění centrální správy IP adresního prostoru s integrovanými nástroji základních síťových služeb (DHCP, DNS), L2 monitoringu a řízení přístupu do sítě (NAC - založený na standardu radius) - s jednotnou uživatelskou správou a následujícím rozsahem funkcionality:

- **Adresní plánování**
- **Monitoring sítě**
- **DHCP server**
- **DNS server**
- **Bezpečnost**
- **Aktivní prvky**
- **Podpora BYOD (WiFi sítě)**

(detailní popis je totožný s níže uvedenou kapitolou)

- **Další funkcionalita:**
  - řídící servery musí podporovat možnost provozu ve virtuálním prostředí (VMware)
  - výkonné servery ve formě fyzických appliancí musí využívat zabezpečený operační systém, být schopné poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti)
  - systém appliancí musí podporovat možnost nasazení v on-line clusteru a podporovat vícenásobnou redundanci
  - systém musí být schopen integrace se systémy pokročilé síťové analýzy (NBA) nebo SIEM
  - SMS brána pro odesílání autentizačních informací uživatelům
  - aktivní spolupráce se stávajícím dohledovým a help-desk systémem kupujícího (RT a ZABBIX)
- **Rozsah nasazení:**
  - centralizovaný systém podporující provozní redundanci služeb L2 monitoringu a DHCP/DNS/NAC
  - celkové množství zařízení – do max. 2000 IP zařízení v síti
  - rozsah nasazení funkcionality: Adresní plánování, Monitoring sítě, DHCP, DNS, Bezpečnost, Aktivní prvky
  - včetně integrace s Microsoft Active Directory
  - možnost budoucího rozšíření funkcionality o podporu BYOD
  - implementace proběhne s využitím standardní implementační metodiky výrobce
- **Výčet stávajících prvků CSMIP:**
  - 1 ks SW – AddNet DDI Server Edition – 2000
  - 1 ks SW – AddNet SIO Multi Vendor module – 2000
  - 1 ks SW – AddNet ES module – 2000
  - 2 ks SW – AddNet Work server
  - 2 ks HW – FireBox appliance 1U Server PLUS

TECHNICKÁ SPECIFIKACE POŽADOVANÝCH ZAŘÍZENÍ KOMPATIBILNÍCH SE STÁVAJÍCÍM PROVOZNĚ-BEZPEČNOSTNÍM DDI/NAC NÁSTROJEM AddNET (což je stávající nástroj kupujícího)

Uvedené specifikace jsou nastaveny jako parametry minimální s ohledem na plnou kompatibilitu a rozšíření.

Kupující požaduje dodat, nainstalovat a uvést do provozu rozšíření následujícího systému Centrální správy a monitoringu IP adresního prostoru včetně všech podpůrných činností pro novou záložní lokalitu.

Systém musí být plně kompatibilní se stávajícím systémem kupujícího popsaným v kapitole Zjednodušený popis stávajícího nástroje CSMIP kupujícího.

Požadujeme nástroj na zajištění centrální správy IP adresního prostoru s integrovanými nástroji základních síťových služeb (DHCP, DNS), L2 monitoringu a řízení přístupu do sítě (NAC - založený na standardu radius) - s jednotnou uživatelskou správou.

Je požadován následující rozsah funkcionality:

Adresní plánování

- nástroj pro návrh a definici IP adresního plánu s možností definice sítí, výběr konkrétní sítě a práce s ní,
- v sítích možnost definice bloků adres, výběry dle bloků adres
- import MAC/IP adres z online monitoringu sítě, automatický výběr správné sítě pro importované adresy
- import/export záznamů do/z adresního plánování v XML nebo CSV formátu
- automatické generování pravidel pro DHCP servery z adresního plánování
- automatické vytváření DNS záznamů z adresního plánování
- možnost vytváření profilů dle sítí, po výběru profilu zobrazení a možnost práce pouze s IP adresami sítí daných profilem
- nástroj pro hromadné práce s definovanými skupinami zařízení a podporu krizového řízení

Monitoring sítě

- monitoring na L2 vrstvě - MAC a IP adres v reálném čase, včetně toho, na kterém fyzickém portu switche se daná MAC adresa nachází, pokud switch tuto možnost poskytuje (na kterém portu kterého switche je připojené zařízení s danou MAC adresou), včetně podpory historie
- dostupnost monitoringu i v lokalitách, kde je přístup přes třetí vrstvu (routované lokality), data musí být online k dispozici přes uživatelské rozhraní na centrální lokalitě
- online sledování a vyhodnocení monitoringu ve formě: povolená dvojice MAC-IP, zakázaná dvojice MAC-IP, nekorektní DHCP MAC-IP, neznámá MAC-IP

- vypsání „mrtvých“ MAC nebo IP adres (adresy, které se v síti nevyskytly např. půl roku), s možností přes uživatelské rozhraní provést vymazání z DHCP, DNS a Radius záznamů a vrácení příslušných IP adres do adresního plánování
- export odmonitorovaných záznamů do XML nebo CSV.

DHCP server

- distribuovaný DHCP systém s možností existence více DHCP serverů na stejné síti (redundance)
- centrální řízení a zakládání pravidel
- podpora redundance řídícího serveru, nezávislé na lokalitě
- uživatelsky definované DHCP volby
- definice adresních skupin, k nim vázané DHCP volby
- možnost vytvoření DHCP pravidla s vazbou více MAC na více IP adres
- pro pravidla možnost definice i statického záznamu (pro danou MAC není přidělovaná adresa DHCP serverem, pouze existuje záznam pro Radius server a monitoring, že daná MAC a IP adresa je na síti platná)
- možnost existence DHCP záznamů jedné MAC adresy ve více různých sítích - v každé síti obdrží daná MAC adresa přesně svou IP adresu z rozsahu dané sítě - cestující uživatelé
- automatické vytvoření/změna/smazání DHCP záznamu při operacích v adresním plánování
- automatická propagace MAC adres z DHCP záznamů v uživatelsky definovaném formátu do Radius serverů pro realizaci dalších bezpečnostních mechanizmů prostřednictvím aktivních prvků sítě (podpora heterogenních aktivních prvků pro 802.1x autentizaci)

DNS server

- centrální řízení a zakládání pravidel
- automatické vytváření A a PTR záznamů z adresního plánování
- centrální řídící server musí mít redundanci nezávislou na lokalitě
- možnost rozdělení zón na vnitřní a vnější pro stejnou zónu, definice vazby na vnitřní nebo vnější zónu dle IP adres (sítí) DNS klientů (klienti ve vnější sítí dostávají odpovědi pouze pro DNS záznamy z vnější zóny, klienti z vnitřní zóny dostávají DNS odpovědi pro vnitřní i vnější zónu).
- replikace zvolených zónových souborů na podřízené DNS server
- možnost automatického vytváření PTR reverzních záznamů při zakládání “A” záznamů
- možnost porovnání DNS z Adresního plánování s DNS záznamy na DNS serveru, včetně automatizovaného nástroje pro řešení rozdílů

Bezpečnost

- řízení přístupu do sítě s využitím 802.1x / MAC autentizace a následné Autorizace (dynamické přidělení VLAN pro zařízení), s využitím integrovaných distribuovaných RADIUS serverů
- systém musí podporovat automatické vytváření záznamů pro 802.1x a jejich automatická propagace do příslušných AAA zařízení z IPAMu
- systém musí podporovat možnost definice politik přístupů pro neznámé zařízení
- systém musí podporovat možnost definice politik přístupů pro důvěryhodná zařízení vyskytující se v jiné části sítě, než do které normálně patří (cestující uživatelé s Notebooky apod.). Pro tato zařízení definovat globální politiky bez nutnosti vytvářet exaktní pravidla pro každé jednotlivé zařízení. Např. důvěryhodná zařízení po úspěšné autentizaci jsou autorizována (automaticky přemístěna) do VLAN definované globální politikou a následně automaticky zasíťovány.
- systém musí podporovat schopnost definovat komplexní síťové politiky, kdy podle výsledku procesu autentizace je aplikována vybraná síťová politika – definované IP a DHCP parametry
- systém musí podporovat krizové řízení – schopnost hromadné deaktivace síťové komunikace pro všechny zařízení mimo vyjmenovanou kritickou infrastrukturu organizace
- podpora krizového řízení – schopnost hromadné deaktivace síťové komunikace pro všechny zařízení mimo vyjmenovanou kritickou infrastrukturu organizace
- uživatelské rozhraní s možností přidělování různých stupňů oprávnění. Audit musí být schopen zaznamenat minimálně kdo, kdy a jaké typy operací v systému prováděl
- sledování incidentů na síti s možností generování bezpečnostních reportů

Aktivní prvky

- automatické zálohování konfigurací aktivních prvků
- sledování výskytu MAC adres na portech s historií pro účely určení, kde se v daném čase vyskytuje nebo vyskytovala MAC adresa.
- automatické repository - informace o verzi firmware, typu zařízení, S/N apod.
- sledování využití portů síťových prvků v čase - detekce nepoužívaných portů
- podpora heterogenního prostředí (podpora více výrobců síťových technologií - switchů)

Podpora BYOD (WiFi sítě)

- podporovaná veškerá funkcionalita rovněž pro mobilní zařízení s přístupem přes Wifi
- podpora samoobslužného rozhraní pro automatizovanou IP správu nových zařízení v síti
- možnost vytváření recepčních zón pro zajištění přístupů návštěv (Guest zóna)

Další požadavky

- řídící servery musí podporovat možnost provozu ve virtuálním prostředí (VMware)

- výkonné servery ve formě fyzických appliancí musí využívat zabezpečený operační systém, být schopné poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti)
- systém appliancí musí podporovat možnost nasazení v on-line clusteru a podporovat vícenásobnou redundanci
- systém musí být schopen integrace se systémy pokročilé síťové analýzy (NBA) nebo SIEM
- kupující požaduje dodání originálních a nových zařízení s požadovanou licencí na jméno kupujícího a podle pravidel výrobce tak, aby bylo možné eskalovat případné závady přímo na lokální technickou podporu výrobce v českém nebo slovenském jazyce.

IMPLEMENTACE

Požadovaný rozsah nasazení:

- centralizovaný systém podporující redundanci řízení a provozu služeb L2 monitoringu a DHCP/DNS/NAC
- celkové množství zařízení – do max. 2000 IP zařízení v síti
- provedení rozšíření upgrade řešení o funkcionalitu podporujících NAC
- provedení donastavení základních síťových služeb podle aktuálních potřeb
- připojení záložní lokality, umožňující lokální redundanci služeb DHCP/DNS/NAC
- rozsah nasazení funkcionality: Adresní plánování, Monitoring sítě, DHCP, DNS, Bezpečnost, Aktivní prvky
- včetně integrace s Microsoft Active Directory
- zajištění detailní implementace NAC služeb spočívající
    - pilotní zprovoznění na testovacím prostředí (MAC auth i plné 802.1x – VoIP, tiskárny, stanice)
    - napojení na MS AD pro plnou 802.1x
    - nastavení základních globálních bezpečnostních politik
    - nastavení mikro segmentačních bezpečnostních politik
    - zaškolení do pokročilých síťových politik
    - intenzivní podpora při nastavování a správě NAC a pokročilých síťových politik po dobu 1 roku
- možnost budoucího rozšíření funkcionality o podporu BYOD
- implementace proběhne s využitím standardní implementační metodiky výrobce
- školení administrátorů a uživatelů

SPECIFIKACE ROZŠÍŘENÍ CSMIP

	Popis	**Množstevní jednotka**	**Počet**
	Novicom software		

AN-ES-2K-upg	AddNet Enterprise Server Edition - 2.000, Upgr. from: AddNet DDI Server Edition, SIO MV module, NAC module	kus	1
AN-ES-2K-HA	AddNet Enterprise Server Edition - 2.000 H/A	kus	1
AN-WS	AddNet Work server	kus	3
	Novicom appliance		
NA-1U-STP	Novicom appliance 1U Standard Plus R18	kus	3
	Implementace		
CON-AN-AS	AddNet - optimalizace aplikačního nastavení, upgrade infrastruktury, integrace a napojení MS AD	MD (8 hodin)	12
CON-AN-AS	AddNet - připojení záložní lokality	MD (8 hodin)	4
CON-AN-AS	AddNet - školení nové funkcionality	MD (8 hodin)	4
CON-AN-AS	AddNet - implementace NAC a pokročilých síťových politik	MD (8 hodin)	20

SERVISNÍ PODPORA

Název
Údržba dodaných HW komponent (maintenance) poskytovaná výrobcem 3 roky
Servisní podpora SLA poskytovaná prodávajícím 3 roky

Údržba dodaných HW komponent – maintenance a následná servisní podpora probíhá v režimu 10 x 5, tzn. v pracovní době 8 – 18 (10 hodin) s reakční dobou do 1 hodiny a opravou u kritických závad (nedostupnost H/A systému) následující pracovní den a u nekritických závad s opravou do 3 pracovních dnů od převzetí požadavku.
Hlášení poruch je prováděno na helpdesk poskytovatele s nepřetržitým provozem.

SPECIFIKACE SERVISNÍ PODPORY

Servisní podpora	**Popis**	**Období**	**Počet**
	Podpora výrobce – stávající i rozšířený CSMIP		
SU-AN-ES-2K	AddNet Enterprise Server Edition - 2.000, Upgr. from: AddNet DDI Server Edition, SIO MV module, NAC module (1 kus)	rok	3
SU-AN-ES-2K-H/A	AddNet Enterprise Server Edition - 2.000 H/A (1 kus)	rok	3
SU-AN-WS	AddNet Work server (3 kusy)	rok	3
SU-NA-1U-STP	Novicom appliance 1U Standard Plus R18 (3 kusy)	rok	3
	Nadstandardní podpora – stávající i rozšířený CSMIP		
CON-SD-8R-8C	Service desk 8hRT - 8hCT	rok	3