[redacted]

POŽADOVANÉ FUNKCIONALITY A VLASTNOSTI	
Obecné minimální požadované vlastnosti a funkce fabric sítě	**Splnění požadavku? Doplněno jak bude splněno/ uvést nabízené zařízení**
Zařízení v rámci Fabric sítě využívají automatizované mechanismy managementu nebo kontroléru pro vytváření virtualizovaných síťových služeb v rámci drátové i bezdrátové infrastruktury.	ANO, Extreme Fabric connect
Datový provoz koncových zařízení neprochází přes kontroléry nebo management, ale je přepínán a směrován přímo v rámci Fabric infrastruktury.	ANO, Extreme Fabric connect
Automatizovaná segmentace koncových zařízení do virtualizovaných L2 segmentů nebo L3 segmentů (dále jen „VRF“) v rámci Fabric sítě, které je možné přidělit staticky nebo dynamicky na základě ověření.	ANO, Extreme Fabric connect
Virtualizované segmenty jsou definované pouze na hranici Fabric sítě bez nutnosti jejich konfigurace na mezilehlých agregačních nebo páteřních prvcích infrastruktury.	ANO, Extreme Fabric connect
Granulární segmentace zabezpečení prostřednictvím uživatelských rolí pro řízení provozu v rámci drátové i bezdrátové infrastruktury.	ANO, Extreme Fabric connect
Automatizovaná konfigurace přístupových portů pro bezpečné připojení uživatelů a jejich zařízení na základě ověření – rozpoznání identity uživatele, zařízení, přidělení role, autorizace apod.	ANO, Extreme Fabric connect
Virtualizované služby v rámci Fabric sítě jsou nezávislé na fyzické topologii. Jsou podporovány virtualizované L2 segmenty a L3 segmenty (VRF) s možností směrování provozu mezi segmenty, ve smyslu Inter-VLAN routing, Inter-VRF routing, VRF leaking apod.	ANO, Extreme Fabric connect
Fabric síť musí podporovat distribuované směrování paketů mezi segmenty pro optimalizaci toku provozu v síti s využitím virtualizace výchozích bran na principu tzv. „Anycast Gateway“.	ANO, Extreme Fabric connect
Dynamické protokoly Fabric sítě, dále jen „Underlay“ nebo „Overlay“, využívají pro řízení provozu a signalizaci virtualizovaných služeb implicitně integrovaných funkcí v rámci protokolů nebo využívají managementu, případně kontroléru Fabric sítě.	ANO, Extreme Fabric connect
Fabric síť musí být jednotná pro drátovou a bezdrátovou síť, tzn., že provoz bezdrátových koncových zařízení nemusí být přenášen či tunelován přes kontrolér bezdrátové sítě, tzn. provoz bezdrátových koncových zařízení je možné ukončit v rámci přístupového přepínače, který poskytuje připojení samotnému přístupovému bodu bezdrátové sítě (tzv. distribuovaný datový model).	ANO, Extreme Fabric connect
Fabric síť musí podporovat přenos multicast provozu, signalizace a směrování multicast provozu je rovněž automatizována prostřednictvím managementu, kontroléru nebo Underlay/Overlay protokolů.	ANO, Extreme Fabric connect
Fabric síť musí podporovat přenos multicast provozu, signalizace a směrování multicast provozu je rovněž automatizována prostřednictvím managementu, kontroléru nebo Underlay/Overlay protokolů.	ANO, Extreme Fabric connect

[redacted]

Fabric síť musí podporovat automatizaci konfigurace QoS v rámci virtualizovaných služeb pro drátová i bezdrátová zařízení prostřednictvím grafického rozraní managementu nebo kontroléru bez nutnosti používat příkazový řádek samotných zařízení.	ANO, Extreme Fabric connect
Řešení musí implementovat virtualizované L2 segmenty a L3 segmenty pro zajištění bezpečné segmentace síťových zařízení v rámci Fabric sítě.	ANO, Extreme Fabric connect
Vytváření virtualizovaných sítí musí být plně automatizováno prostřednictvím managementu nebo kontroléru Fabric sítě, případně s využitím implicitní automatizace v Overlay a to bez nutnosti používat příkazový řádek samotných zařízení.	ANO, Extreme Fabric connect
Přiřazení příslušné virtualizované sítě nebo segmentu je koncovému zařízení provedeno automatizovaně na základě ověření a přidělení příslušné role.	ANO, Extreme Fabric connect
Vytváření virtualizovaných segmentů a přiřazení rolí musí být možné v grafickém rozhraní managementu nebo kontroléru Fabric sítě a nesmí vyžadovat manuální konfigurační zásah.	ANO, Extreme Fabric connect
Vytváření rolí pro segmentaci sítě je možné prostřednictvím managementu nebo kontroléru Fabric sítě, který následně konfiguruje systém řízení přístupu do sítě NAC na základě příslušné konfigurace.	ANO, Extreme Fabric connect
Management nebo kontrolér Fabric sítě musí zobrazit používané aplikace, protokoly a porty používané v rámci síťové infrastruktury pro možnou optimalizaci rolí a pro podrobnější segmentaci sítě.	ANO, Extreme Fabric connect
Navrhované řešení Fabric sítě využívá některou ze standardizovaných metod zapouzdření provozu koncových zařízení do jednotlivých segmentů.	ANO, Extreme Fabric connect
Navrhované řešení Fabric sítě podporuje šifrování na L2 vrstvě s využitím protokolu MACsec.	ANO, Extreme Fabric connect
Management nebo kontrolér musí podporovat automatizované řízení přístupu do Fabric sítě na všech přepínačích a bezdrátových přístupových bodech s využitím různých typů 802.1X a MAC-Auth a to bez nutnosti použít příkazový řádek.	ANO, Extreme Fabric connect
Management nebo kontrolér musí podporovat automatizované řízení přístupu návštěv do Fabric sítě na všech přepínačích a bezdrátových přístupových bodech s využitím webového ověření a to bez nutnosti použít příkazový řádek.	ANO, Extreme Fabric connect
Navrhované řešení Fabric sítě musí podporovat integraci s prvky třetích stran za účelem automatizované předání identity uživatele nebo koncového zařízení, např. Single-Sign-On s Next-Generation Firewally, za účelem další segmentace zařízení a jejich síťového provozu.	ANO, Extreme Fabric connect
Management nebo kontrolér Fabric sítě podporuje integraci s Next-Generation Firewally pro monitorování síťového provozu, detekci incidentů a automatizovanou izolaci postižených koncových zařízení.	ANO, Extreme Fabric connect
Navrhované řešení poskytuje nástroj pro centrální správu sítě v hierarchické struktuře založenou na profilech, lokalitách a rolích.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje centrální správu bezdrátových sítí prostřednictvím integrace bezdrátového kontroléru s managementem nebo kontrolérem Fabric sítě.	ANO, Extreme Fabric connect

[redacted]

Navrhované řešení umožňuje centralizované nastavení parametrů provozního a bezpečnostního monitoringu Fabric sítě.	ANO, Extreme Fabric connect
Kontrolér nebo management musí poskytovat funkce pro automatizované sestavení Underlay Fabric sítě ve spravované lokalitě.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje automatizované vyhledání a připojení nových sítových přepínačů zapojených v lokalitě k jednomu nebo více podporovaným a spravovaným přepínačům, tvz. „Seed“ přepínačům.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje automatickou alokaci IP adresy pro management rozhraní nově přidaného přepínače do Underlay Fabric sítě s využitím automatizace kontroléru nebo managementu, nebo s využitím implicitní automatizace v Underlay.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje další konfigurace přidávaných přepínačů do Underlay Fabric sítě s využitím automatizovaných postupů, skriptů nebo workflow.	ANO, Extreme Fabric connect
Navrhované řešení podporuje automatizované zavedení nově přidaných zařízení do inventáře kontroléru nebo managementu Fabric sítě, včetně archivace jejich konfigurací.	ANO, Extreme Fabric connect
Navrhované řešení podporuje konfiguraci zařízení s využitím v rámci Underlay s využitím vlastní šablony nebo skriptu v případě, že není navrhovaná konfigurace vhodná či žádoucí.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje snadné rozšíření Underlay Fabric sítě o další přepínače přes tzv. „Zero Touch Provisioning“.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje definici rolí jednotlivých zařízení přes grafické prostředí kontroléru nebo managementu Fabric sítě.	ANO, Extreme Fabric connect
Součástí navrhovaného řešení managementu nebo kontroléru musí být systém pro řízení přístupu do sítě s možností výběru různých metod ověřování s automatizovaným přidělením služby nebo role pro připojené zařízení.	ANO, Extreme Fabric connect
Součástí navrhovaného řešení managementu nebo kontroléru je nástroj pro vytváření a aktivaci segmentů v rámci Fabric sítě. Součástí navrhovaného řešení managementu nebo kontroléru je možnost definice a aktivace segmentů pro používané bezdrátové sítě v rámci Fabric sítě.	ANO, Extreme Fabric connect
Součástí navrhovaného řešení managementu nebo kontroléru je nástroj pro nastavení řízení multicast provozu ve Fabric síti.	ANO, Extreme Fabric connect
Navrhované řešení umožňuje nastavení specifické konfigurace portu, které jsou odlišné od centrální politiky nebo šablony.	ANO, Extreme Fabric connect
Navrhované řešení podporuje migraci zařízení ze stávající infrastruktury do Fabric sítě, IP rozsah může být rozprostřen mezi stávající infrastrukturou a Fabric sítí. 4 letá licence pro managementu switchů a analytické nástroje **(pro dodávaná zařízení)**	ANO, Extreme Fabric connect
4 letá licence pro 4 stávající zařízení zadavatele (tyto 4 licence nejsou zamýšlené pro nově pořizovaná zařízení v rámci této zakázky)	ANO, ExtremeCloud IQ Navigator

[redacted]

Vlastnosti z pohledu síťového managementu	Splnění požadavku? Doplněno jak bude splněno/ uvést nabízené řešení
Licenční pokrytí a podpora	
Požadovaný počet spravovaných zařízení v rámci centrálně řízené infrastruktury (minimálně 8 zařízení)	ANO, ExtremeCloud IQ Pilot
Licence, záruka, podpora, aktualizace SW a přístup k novým funcionalitám na dobu minimálně 4roky	ANO, ExtremeCloud IQ Pilot
Obecné vlastnosti	
Požadovaný formát zařízení VA (virtual appliance) pro server na platformě vmware nebo hyper-v nebo kvm	ANO
Plnohodnotná klientská část podporovaná na operačních systémech Linux, Windows i OS X	ANO
Plnohodnotný přístup přes HTML pomocí webového prohlížeče (minimálně Edge, Firefox, Chrome)	ANO
Víceúrovňová práva přístupu, podpora paralelní práce více uživatelů	ANO
Podpora autentizace operátorů pomocí LDAP, Radius	ANO
Možnost napojení on-premise managementu do cloudového managementu výrobce	ANO
RBAC = rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám	ANO
Podpora IPv4 i IPv6	ANO
Podpora SNMPv1, SNMPv2, SNMPv3, AES pro SNMPv3 (netSNMP)	ANO
Podpora hromadného skriptování pomocí telnet i ssh	ANO
Periodická záloha vlastní konfigurace	ANO
Import MIB třetích stran	ANO
Záloha a obnovení konfigurace, aktualizace firmware	ANO
Nastavení syslog a trap cílů	ANO
Zobrazení a nastavení data a času, zobrazení uptime	ANO
Detekce a zobrazení L2 topologie sítě formou mapy	ANO
Vyhledávání koncových zařízení na síti přes IP, Subnet, MAC, login	ANO
Načítání informací z MIB – STP, utilizace, Inventář, VLAN, LACP, MSTP, utilizace portů, možnost definice vlastních tabulek/pohledů	ANO
Export a periodický export zobrazovaných hodnot minimálně do csv	ANO
Vizualizace zařízení (porty, sloty)	ANO
Centrální management bezpečnostních přístupových profilů	
Bezpečnostní přístupový profil je kombinace minimálně VLAN, L2-L4 ACL, L2-L4 QoS pravidel	ANO
Vytváření, správa, rušení bezpečnostních přístupových profilů centrálně s automatickou distribucí do aktivních prvků i WiFi sítě	ANO
Aplikování bezpečnostního přístupového profilu na port aktivního prvku	ANO
SNMP trap server, Syslog server, BootP server	ANO
Podpora vyčítání a zobrazování RMON	ANO
Možnost reakce na přijatý trap a syslog, výpadek konektivity pomocí technik email, trap, syslog, spuštění skriptu	ANO

[redacted]

Network discovery na základě IP rozsahu, rekurzivního dotazování sousedů	ANO
Archivace konfigurací	ANO
Hromadná záloha konfigurace ze spravovaných zařízení pomocí TFTP, SCP, FTP	ANO
Automatická záloha konfigurace spravovaných zařízení minimálně jednou, denně, týdně, při startu	ANO
Inventarizace sériových čísel jednotlivých komponent (zdroje, moduly)	ANO
Porovnávání rozdílných konfigurací se zvýrazněním rozdílů	ANO
Obnovení konfigurace	ANO
Klonování konfigurace z jednoho prvku na druhý	ANO
Vytváření, správa a aplikování konfiguračních šablon na aktivní prvky	ANO
Reporty	
Generování reportu na vyžádání	ANO
Naplánování odeslání reportu do emailu (hodinově, denně, týdně, měsíčně)	ANO
Porty s nejvyšším vytížením, chybovostí, nejnižší dostupností	ANO
Nejdéle nevyužívané porty	ANO
Prvky s nejvyšším vytížením byte/packet, vytížení CPU, vytížením paměti	ANO
Nástroj pro Helpdesk	
Nalezení hledané MAC adresy v síti bez ohledu na to, zda koncové zařízení bylo autorizováno	ANO
Nalezení portu, kde je připojena hledaná IP adresa (vyhledávané koncové zařízení nemusí být autorizováno	ANO
Zobrazení aktuálního i historického vytížení portu	ANO
Automatizace instalace aktivních prvků	
Na nově přidaný aktivní prvek do sítě je automaticky (bez zásahu obsluhy) nainstalován referenční firmware	ANO
Na nově přidaný aktivní prvek do sítě jsou automaticky (bez zásahu obsluhy) distribuovány konfigurace VLAN, SYSLOG a SNMP trap cílů	ANO
Na nově přidaný aktivní prvek do sítě jsou automaticky (bez zásahu obsluhy) distribuovány konfigurace bezpečnostních profilů	ANO
Na nově přidaný aktivní prvek do sítě jsou automaticky (bez zásahu obsluhy) distribuovány konfigurace Radius serverů	ANO
Automatizace pracovních postupů	
Definice akcí, které je možné spustit v určeném pořadí (akcí může být minimálně CLI skript, SNMP komunikace, volání API či spuštění skriptu na management stanici)	ANO
Mezi akcemi je možno používat podmínečné větvení na základě výsledku předchozí akce	ANO
Mezi akcemi je možno používat podmínečné větvení na základě hodnoty proměnné	ANO

[redacted]

Vlastnosti z pohledu ověřování uživatelů	Splnění požadavku? Doplněno jak bude splněno/ uvést nabízené řešení
Architektura	Extreme Networks NAC
Plná integrace s dodávaným síťovým managementem (zařízení není nutno zadávat zařízení vícekrát, informace jsou automaticky sdíleny)	ANO
Požadovaný formát zařízení VA (virtual appliance) pro server na platformě vmware nebo hyper-v nebo kvm	ANO
Požadovaný počet ověřených zařízení (minimálně 1000 zařízení)	ANO
Plnohodnotná klientská část podporovaná na operačních systémech Linux, Windows i OS X	ANO
Plnohodnotný přístup přes HTML pomocí webového prohlížeče (minimálně Edge, Firefox, Chrome)	ANO
Víceúrovňová práva přístupu, podpora paralelní práce více uživatelů	ANO
Podpora autentizace pomocí LDAP, Radius	ANO
RBAC (rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám)	ANO
Konfigurace, monitoring i reporting systému přes HTTPs rozhraní ve standardním webovém prohlížeči (minimálně Edge, Firefox, Chrome)	ANO
Systém musí být schopen výměny informací s dalšími systémy (otevřené a dokumentované API).	ANO
Při dotazu na MAC či IP či hostname poskytnout informace: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav připojen/odpojen, health check, první a poslední výskyt zařízení	ANO
Na základě MAC vynutit reautentizaci uživatele	ANO
Změnit koncovému zařízení přístupový profil (přesun do karantény, z karantény, do jakéhokoliv jiného bezpečnostního přístupového profilu)	ANO
Změnit uživateli přístupový profil (přesun do karantény, z karantény, do jakéhokoliv jiného bezpečnostního přístupového profilu)	ANO
Odpojit koncové zařízení ze sítě	ANO
Vytvořit, aktivovat a deaktivovat uživatelský účet (jméno a heslo do lokální databáze)	ANO
Integrace se stávající adresářovou službou pomocí LDAPs a Radius protokolů	ANO
Centrální správa (centrální místo pro konfiguraci i dohled všech komponent)	ANO
Vysoká dostupnost (Active - Active)	ANO
Autentizace	
Možnost autentizovat zařízení minimálně pomocí 802.1X, MAC a webovým portálem	ANO
Možnost autentizovat a autorizovat vice identit na jednom portu (telefon, PC, virtuální stroje)	ANO
IEEE 802.1X minimálně EAP-TLS, EAP-TTLS, EAP-MD5, EAP-PEAP, EAP-LEAP, EAP-RSA a EAP-SIM	ANO
MAC autentizace minimálně PAP, CHAP a EAP-MD5	ANO

[redacted]

Vnitřní databáze MAC včetně podpory bitového maskování MAC adres	ANO
Autentizace vůči nadřazenému Radius serveru	ANO
Autentizace vůči nadřazenému LDAP serveru	ANO
Autentizace vůči Microsoft Entra ID	ANO
Autentizace vůči vnitřní databázi	ANO
Použití různých autentizačních autorit, minimálně dle lokality kde se uživatel nachází, dle uživatelského jména a dle domény	ANO
Autorizace	
Systém musí být schopen aplikovat rozdílné bezpečnostní přístupové profily minimálně na základě kombinace všech těchto podmínek: MAC, OUI, port/přepínač, den v týdnu, čas, příslušnost uživatele i počítače v LDAPu a Radiusu, typu autentizace, typu koncového zařízení a typu operačního systému koncového zařízení	ANO
Systém musíbýt schopen dynamicky přidělit VLANu a ACL pro jednotlivá koncová zařízení	ANO
Systém musí být schopen dynamicky přidělit QoS pro jednotlivá koncová zařízení (802.1p a DSCP/ToS hodnoty rozdílné pro rozdílná zařízení)	ANO
Systém musí podporovat využití CoA (RFC 3576)	ANO
Systém musí umožnit uživatelům registraci vlastních zařízení bez zásahu administrátora (onboarding)	ANO
Přístup pro hosty	
Systém musí poskytovat vícejazyčný web portál pro hosty	ANO
Portál musí být možno graficky upravovat	ANO
Portál musí rozpoznat typ prohlížeče a dle toho nabídnout optimalizovaný obsah pro identifikovaná zařízení (smartphone, tablet, PC)	ANO
Systém musí být schopen uživateli zobrazit rozdílné portály dle lokality, kde se uživatel aktuálně nachází (dle SSID, přepínače a AP)	ANO
Možnost definice délky platnosti účtu pro hosty s minimální časovou přesností 1 minuta	ANO
Systém musí poskytovat specializovaný přístup pro hosty, a to minimálně v následujících režimech:	ANO
Registrace bez ověření	ANO
Registrace ověřením přes SMS a email	ANO
Registrace autorizací zaměstnancem (sponzorovaný přístup)	ANO
Registrace pomocí sociálních sítí (Facebook, Microsoft, Google)	ANO
Reporting a helpdesk	
Systém musí být schopen zobrazit o všech zařízeních v síti minimálně následující informace: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav připojen/odpojen, health check, první a poslední výskyt zařízení	ANO
Systém musí být schopen vyhledat zařízení minimálně na základě následujících kritérií: MAC, IP, hostname, typ zařízení, username, port / SSID+AP, aktivní prvek, stav připojení připojen/odpojen, risk status, čas prvního a posledního výskytu	ANO

[redacted]

Systém musí být schopen udržovat minimálně 30-ti denní historii o kterémkoliv zvoleném zařízení v síti, a to v minimálně v následujícím rozsahu: IP, hostname, typ zařízení, uživatelské jméno, port /SSID+AP, aktivní prvek, stav připojen/odpojen, health check	ANO
Systém musí být schopen zobrazit informace o aktuálním i historickém stavu, statistikách, vytížení aktivního prvku/AP kde je hledané zařízení připojeno	ANO
Systém musí umožňovat export informací do externího úložiště (Log management, SIEM) v uživatelsky definovaném formátu, a to v minimálně v následujícím rozsahu: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav připojen/odpojen, časová známka	ANO
Systém musí být schopen vygenerovat email při změně stavu zařízení	ANO

Vlastnosti z pohledu monitoringu aplikací	**Splnění požadavku? Doplněno jak bude splněno/ uvést nabízené řešení**
Architektura	ANO, ExtremeCloud IQ Pilot
Plná integrace s dodávaným síťovým managementem (zařízení není nutno zadávat zařízení vícekrát, informace jsou automaticky sdíleny)	ANO
Požadovaný formát zařízení VA (virtual appliance) pro server na platformě vmware nebo hyper-v nebo kvm	ANO
Plnohodnotná klientská část podporovaná na operačních systémech Linux, Windows i OS X	ANO
Plnohodnotný přístup přes HTML pomocí webového prohlížeče (minimálně Edge, Firefox, Chrome)	ANO
Víceúrovňová práva přístupu, podpora paralelní práce více uživatelů	ANO
Podpora autentizace pomocí LDAP, Radius	ANO
RBAC (rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám)	ANO
Konfigurace, monitoring i reporting systému přes HTTPs rozhraní ve standardním webovém prohlížeči	ANO
Funkcionalita	
Analýza komunikace procházející přes aktivní prvek na 2 až 7 vrstvu OSI modelu. Požadovaná funkcionalita musí být v reálném čase dostupná na právě všech portech dotčeného aktivního prvku.	ANO
Schopnost zobrazit a detekovat nejvíce vytížené aplikace (minimálně z pohledu množství toků a počtu klientů)	ANO
Konfigurovatelný dashboard, obsahující například informace typu „použité aplikace v síti“, „systémy a klienti s největším přenosem dat“, „počet aktuálních klientů a serverů v síti“, „žebříček využitelnosti aplikací dle počtu klientů, datových toků a množství přenesených dat“	ANO
Způsob vizualizace pomocí grafů, map a tabulek	ANO
Analýza a reportování zpoždění na úrovni sítě (Network Round Trip Delay pro aplikaci, uživatele a stanici)	ANO

[redacted]

Analýza propustnosti a zpoždění jedné aplikace i skupiny aplikací	ANO
Analýza využití zdrojů na základě aplikace i na základě klienta	ANO
Možnosti zobrazení v rámci managementu	
Zobrazení klientů jménem stanice i uživatele	ANO
Zobrazení klientů dle lokalit, kde jsou připojeni do sítě	ANO
Upozornění a alarmy	
Automatické upozornění na překročení nastavených prahových hodnot	ANO
Schopnost exportu L7 informací do externí databáze pro dlouhodobou archivaci	ANO