Příloha č. 1 zadávací dokumentace – technické podmínky a akceptační testy

Veřejná zakázka: Rámcové smlouvy na dodávky ICT komponent

Část C - Firewall a proxy servery

**Firewall a web filter**

##### 1. Parametry předmětu veřejné zakázky - individuální

**Komodita 1 - Firewall a web filter pro 50 souběžných uživatelů**

1. Rozhraní 4 x 1000BASE-T, HW platforma
2. Výkonnost zařízení:
   1. Počet souběžných spojení s 50 ACL pravidly na rozhraní 200 000
   2. Počet nových spojení za vteřinu s 50 ACL pravidly na rozhraní – 2 000
   3. Počet odbavených http požadavků za vteřinu s odpovědí o velikosti 8kB na rozhraní firewallu s webovým filtrem při zapnutí kategorizace (2 kategorie) a HTTPS inspekce - 800
3. Definice rozhraní LAN, WAN a DMZ včetně definice 4 VLAN
4. Licenční pokrytí pro 50 souběžně pracujících uživatelů
5. Grafické rozhraní pro správu přes zabezpečený kanál (např. HTTPS, SSH) a vzdálený šifrovaný přístup na CLI
6. Management s možností definice administrátorských rolí a účtů
7. SNMP – vyčítání stavu zařízení (počet aktivních session, provoz na rozhraních, počet aktivních rozhraní, …)
8. Vzdálené vyčítání informací o stavu zařízení (verze firmware, výkonové parametry, celkové zdraví zařízení, …. ) Integrovatelné do centrálního konzole/dohledu
9. Aplikování nových pravidel bez ukončení běžících session (firewall i webová proxy)
10. Synchronizace času přes NTP nebo obdobné technické řešení, NTP server
11. Zálohování konfigurace, upload konfigurace, definice cíle a frekvence záloh
12. DHCP server včetně přehledu o přidělených adresách, statické rezervace IP
13. Zasílání NETFLOW v9 nebo IPFIX včetně informace o překladech IP adres se vzorkem max. 1:10 na min. jeden kolektor
14. Plnohodnotná podpora IPv4 a IPv6 - dual-stack
15. Statické routování
16. Stavový paketový filter, ACL filter, Antispoofing, nastavení ratelimit (IP adresa, protokol)
17. Obrana před útoky min. DNS Query Flood, SYN Flood, UDP Flood, ICMP Flood, Ping of Death, Smurf
18. Zdrojový NAT s Port Address Translation (PAT), cílový NAT s PAT, Statický NAT, Dynamický NAT, NAT 1:1, redirect
19. L7 aplikační kontrola - blokování streamovaného obsahu (audio, video), blokování tunelování (např. přenos souborů přes SKYPE, …), blokování P2P sítí, blokování sociálních sítí
20. Aplikační služby (proxy)- H.323, FTP, DNS s validací přes DNSSec
21. VPN (např. IPSec, OpenVPN, SSL), site-to-site, client-to-site, min. 5 souběžných session, podpora OS Windows, Linux, Android, iOS, včetně potřebných licencí
22. Autentizace uživatelů webproxy oproti MS Active directory, LDAP, lokální databáze uživatelů (protokol Kerberos nebo NTLM) bez nutnosti instalace klientského SW na stanici,
23. Výjimky na autentizaci webproxy dle zdrojové nebo cílové IP
24. Nasazení webového filtru v transparentním nebo netransparentním režimu pro HTTP
25. Kontrola HTTPS provozu, ověřování certifikátu na proxy
26. Výjimky z HTTPS inspekce na určené zdrojové IP a uživatele, servery nebo kategorie
27. Kategorizace webových domén dle obsahu v počtu min. 50ks, kategorizační databáze uložena v zařízení s možností pravidelného automatického update z internetu, databáze kategorií v rámci dodávky
28. Samostatné kategorie domén pro www se škodlivými kódy a P2P
29. Politika přístupu uživatele na služby definovaná dle času, kategorií, cílové adresy, uživatele, skupiny uživatelů
30. Definice vlastní kategorie serverů (vlastní seznam serverů pro nastavení pravidel)
31. Definice black/white listů (uživatel, skupina, IP adresa)
32. Reklamace chybného URL kategorizačního záznamu pomocí webového formuláře, zpětná vazba, rychlost reakce na ruční hlášení do 48h v pracovní dny
33. Blokování přístupu do určených kategorií serverů
34. Aktualizace webového filtru o nezařazené domény z webového provozu v pracovní dny do 48h
35. Interface pro protokol ICAP na zapojení externího antiviru (např. ClamAV)
36. Antivirové řešení pro kontrolu stahovaného obsahu přes webovou proxy
    1. skenování určených typů souborů
    2. skenování archivů, instalačních balíčku, OLE objektů
    3. blokování přístupu na infikovaný/podezřelý objekt, informování uživatele
    4. odstranění infekce (pokud to je možné)
    5. konfigurace reportů, logování událostí
37. Monitoring provozu, statistiky provozu, periodické reporty o provozu, údaje o úspěšné kategorizaci provozu přes filter (http i https), nástroj na prohledávání logů, log aktivity správce zařízení
38. Logování na externí server přes protokol Syslog (aktivita správce, firewall log, VPN log, …)
39. Perpetual licenční pokrytí veškeré požadované funkcionality včetně maintenace dle rámcové smlouvy
40. Navýšení počtu uživatelů o 30% formou doplnění licencí - bez dalších změn HW a SW
41. Dokumentace řešení, zaškolení obsluhy v počtu 2 pracovníků v rozsahu 4 hodin
42. Záruční doba na HW dle rámcové smlouvy (v případě volby HW appliance)

**Nepovinné požadavky (zohledněno při hodnocení):**

1. Nastavení přenosového pásma pro uživatele u webové proxy (garantované pásmo, maximální pásmo, řízení provozu dle definovaných politik),
2. Definice u webproxy důvěryhodných CA, podpis nedůvěryhodných CA, rozlišení typu chyb (expirace certifikátu, chybná doména, …)
3. Zapnutí informace pro uživatele o dekrypci provozu u webového filtru v případě potřeby a interace uživatele o převzetí informace
4. Upozornění a blokování kategorií serverů, podmíněné zpřístupnění na omezenou dobu (pro správce i uživatele)

**Komodita 2 - Firewall a web filter pro 50 souběžných uživatelů**

Technické zadání musí splňovat všechny požadavky pro komoditu 1, kromě bodu 1. Bod 1 zadávací dokumentace je nahrazen následujícím textem:

1. Rozhraní 4 x 1000BASE-T, virtuální appliance pro VMWare ESX nebo HyperV

**Komodita 3 - Firewall a web filter pro 300 souběžných uživatelů**

Firewall včetně webového filteru – minimální požadavky :

1. Rozhraní 8x 1000BASE-T, HW platforma provedení rackmount 19“ a redundantní zdroje napájení
2. Možnost provozu v konfiguraci cluster v případě zakoupení druhého node
3. Výkonnost zařízení:
   1. Počet souběžných spojení s 50 ACL pravidly na rozhraní 1 000 000
   2. Počet nových spojení za vteřinu s 50 ACL pravidly na rozhraní – 13 000
   3. Počet odbavených http požadavků za vteřinu s odpovědí o velikosti 8kB na rozhranní firewallu s webovým filtrem při zapnutí kategorizace (2 kategorie) a HTTPS inspekce - 4000
4. Definice rozhraní LAN, WAN a DMZ včetně definice 8 VLAN, konfigurace 2 ethernet rozhraní pro jednu logickou linku v módu Active/Standby
5. Licenční pokrytí pro 200 souběžně pracujících uživatelů
6. Grafické rozhraní pro správu přes zabezpečený kanál (např. HTTPS, SSH) a vzdálený šifrovaný přístup na CLI
7. Management s možností definice administrátorských rolí a účtů
8. SNMP, SNMPv3 protokol – vyčítání stavu zařízení (počet aktivních session, provoz na rozhraních, počet aktivních rozhraní, …)
9. Vzdálené vyčítání informací o stavu zařízení (verze firmware, výkonové parametry, celkové zdraví zařízení, …. ) Integrovatelné do centrálního konzole/dohledu
10. Aplikování nových pravidel bez ukončení běžících session (firewall i webová proxy)
11. Synchronizace času přes NTP nebo obdobné technické řešení
12. Zálohování konfigurace, upload konfigurace
13. Zasílání NETFLOW v9 nebo IPFIX včetně informace o překladech IP adres se vzorkem max. 1:10 na min. jeden cíl
14. Plnohodnotná podpora IPv4 a IPv6 - dual-stack
15. Statické routování, protokol OSPF,
16. Policy routing na základě určení zdrojové IP, cílové IP, řízení směrování přes 2 poskytovatele připojení do sítě Internet
17. Stavový paketový filter, ACL filter, Antispoofing, nastavení ratelimit (IP adresa, protokol)
18. Obranu před útoky min. DNS Query Flood, SYN Flood, UDP Flood, ICMP Flood, Ping of Death, Smurf
19. Zdrojový NAT s Port Address Translation (PAT), cílový NAT s PAT, Statický NAT, Dynamický NAT, NAT 1:1, redirect
20. L7 aplikační kontrola - blokování streamovaného obsahu (audio, video), blokování tunelování (např . přenos souborů přes SKYPE, …), P2P sítí, sociálních sítí
21. Aplikační služby (proxy)- H.323, FTP, SIP, DNS s validací přes DNSSec
22. Nastavení přenosového pásma pro uživatele (garantované pásmo, maximální pásmo, řízení provozu dle definovaných politik), QoS
23. VPN (např. IPSec, OpenVPN, SSL) site-to-site, client-to-site, min. 10 souběžných session, podpora OS Windows, Linux, Android, iOS, včetně potřebných licencí
24. Možnost doplnění VPN s dvoufázovou SMS autorizaci pro uživatele
25. Autentizace uživatelů oproti MS Active directory, LDAP nebo lokální databáze uživatelů (protokol Kerberos nebo NTLM) bez nutnosti instalace klientského SW na stanici, licenční pokrytí pro variantu klientského SW, transparetní autentizace
26. Výjimky na autentizaci dle zdrojové nebo cílové IP
27. Přidělování šířky pásma v závislosti na zdrojové/cílové IP, www kategorií
28. Nasazení webového filtru v transparentním nebo netransparentním režimu pro http
29. Výjimky z HTTPS inspekce na určené zdrojové IP, cílové servery nebo kategorie
30. Kontrola HTTPS provozu, ověřování certifikátu na proxy
31. Kategorizace webových domén dle obsahu v počtu min. 50ks, kategorizační databáze nezávislá na online službě nebo cloudu, databáze kategorií v rámci dodávky
32. Samostatné kategorie domén pro www se škodlivými kódy a P2P
33. Politika přístupu uživatele na služby definovaná dle času, kategorií, cílové adresy, uživatele, skupiny uživatelů
34. Definice vlastní kategorie serverů
35. Kategorizace webových stránek podle celé URL adresy
36. Ověřování přenášených souborů u webové proxy na základě MIME type i CONTENT type, nastavení pravidla pro zákaz přenosu
37. Detekování typů přenášených souborů v HTTP/HTTPS komunikaci
38. Definice black/white listů (uživatel, skupina, adresa)
39. Reklamace chybného záznamu pomocí webového formuláře, zpětná vazba, rychlost reakce na ruční hlášení do 48h v pracovní dny
40. Blokování přístupu do určených kategorií serverů
41. Aktualizace webového filtru o nezařazené domény z webového provozu v pracovní dny do 48h
42. Interface pro protokol ICAP na zapojení externího antiviru (např. ClamAV)
43. Antivirové řešení pro kontrolu stahovaného obsahu přes webovou proxy
    1. skenování určených typů souborů
    2. skenování archivů, instalačních balíčku, OLE objektů
    3. blokování přístupu na infikovaný/podezřelý objekt, informování uživatele
    4. odstranění infekce (pokud to je možné)
    5. konfigurace reportů, logování událostí
44. Monitoring provozu, statistiky provozu, periodické reporty o provozu, údaje o úspěšné kategorizaci provozu přes filter (http i https), nástroj na prohledávání logů firewallu i webové proxy, log aktivity správce zařízení
45. Nastavení doby pro uchování záznamů na lokálním úložišti logů
46. Logování na externí server přes protokol Syslog (aktivita správce, firewall log, …)
47. Zachycení provozu pro následnou analýzu (dump provozu pro následnou analýzu např. ve Wiresharku)
48. Perpetual licenční pokrytí veškeré požadované funkcionality včetně maintenance dle rámcové smlouvy
49. Navýšení počtu uživatelů o 30% formou doplnění licencí - bez dalších změn HW a SW
50. Dokumentace řešení, zaškolení obsluhy v počtu 2 osob v rozsahu 4 hodiny
51. Záruční doba na HW dle rámcové smlouvy (v případě volby HW appliance)

**Nepovinné požadavky – (zohlednění při hodnocení)**

1. Omezení délky trvání spojení maximálním množstvím přenesených dat (není nutné u navázaných session)
2. Zapnutí informace pro uživatele o dekrypci v případě potřeby a interace uživatele o převzetí informace
3. Definice důvěryhodných CA, podpis nedůvěryhodných CA, rozlišení typu chyb (expirace certifikátu, chybná doména, slabý šifrovací klíč …), podmíněné zpřístupnění na omezenou dobu
4. Upozornění a blokování kategorií serverů, podmíněné zpřístupnění na omezenou dobu (upozornění pro správce i uživatele)

**Komodita 4 - Firewall a web filter pro 300 souběžných uživatelů**

Technické zadání musí splňovat všechny požadavky pro komoditu 3, kromě bodu 1. Bod 1 zadávací dokumentace je nahrazen následujícím textem:

1. Rozhraní 8 x 1000BASE-T, virtuální appliance pro VMWare ESX nebo HyperV

**Komodita 5 - Firewall a web filter pro 1000 souběžných uživatelů**

Firewall včetně webového filteru – minimální požadavky :

1. Rozhraní 12x 1000BASE-T, HW platforma provedení rackmount 19“ a redundantní zdroje napájení
2. Možnost provozu v konfiguraci cluster v případě zakoupení druhého node
3. Výkonnost zařízení:
   1. Počet souběžných spojení s 50 ACL pravidly na rozhraní 2 000 000
   2. Počet nových spojení za vteřinu s 50 ACL pravidly na rozhraní – 20 000
   3. Počet odbavených http požadavků za vteřinu s odpovědí o velikosti 8kB na rozhraní firewallu s webovým filtrem při zapnutí kategorizace (2 kategorie) a HTTPS inspekce - 8000
4. Definice rozhraní LAN, WAN a DMZ včetně definice 32 VLAN, konfigurace 2 ethernet rozhraní pro jednu logickou linku v módu Active/Standby
5. Licenční pokrytí pro 200 souběžně pracujících uživatelů
6. Grafické rozhraní pro správu přes zabezpečený kanál (např. HTTPS, SSH) a vzdálený šifrovaný přístup na CLI
7. Management s možností definice administrátorských rolí a účtů
8. SNMP, SNMPv3 protokol – vyčítání stavu zařízení (počet aktivních session, provoz na rozhraních, počet aktivních rozhraní, …)
9. Vzdálené vyčítání informací o stavu zařízení (verze firmware, výkonové parametry, celkové zdraví zařízení, …. ) Integrovatelné do centrálního konzole/dohledu
10. Aplikování nových pravidel bez ukončení běžících session (firewall i webová proxy)
11. Synchronizace času přes NTP nebo obdobné technické řešení
12. Zálohování konfigurace formou textového formátu, upload konfigurace
13. Historie konfiguračních změn, porovnávání verzí konfigurací
14. Zasílání NETFLOW v9 nebo IPFIX včetně informace o překladech IP adres se vzorkem max. 1:10 na min. jeden cíl
15. Plnohodnotná podpora IPv4 a IPv6 - dual-stack
16. Statické routování, protokol OSPF, BGP
17. Policy routing na základě určení zdrojové IP, cílové IP, řízení směrování přes 2 poskytovatele připojení do sítě Internet
18. Stavový paketový filter, ACL filter, Antispoofing, nastavení ratelimit (IP adresa, protokol)
19. Obranu před útoky min. DNS Query Flood, SYN Flood, UDP Flood, ICMP Flood, Ping of Death, Smurf
20. Zdrojový NAT s Port Address Translation (PAT), cílový NAT s PAT, Statický NAT, Dynamický NAT, NAT 1:1, redirect
21. L7 aplikační kontrola - blokování streamovaného obsahu (audio, video), blokování tunelování (např . přenos souborů přes SKYPE, …), P2P sítí, sociálních sítí
22. Aplikační služby (proxy)- H.323, FTP, SIP, DNS s validací přes DNSSec
23. Nastavení přenosového pásma pro uživatele (garantované pásmo, maximální pásmo, řízení provozu dle definovaných politik), QoS
24. VPN (např. IPSec, OpenVPN, SSL) site-to-site, client-to-site, min. 10 souběžných session, podpora OS Windows, Linux, Android, iOS, včetně potřebných licencí
25. Možnost doplnění VPN s dvoufázovou SMS autorizaci pro uživatele
26. Autentizace uživatelů oproti MS Active directory, LDAP nebo lokální databáze uživatelů (protokol Kerberos nebo NTLM) bez nutnosti instalace klientského SW na stanici, licenční pokrytí pro variantu klientského SW, transparetní autentizace
27. Výjimky na autentizaci dle zdrojové nebo cílové IP
28. Přidělování šířky pásma v závislosti na zdrojové/cílové IP, www kategorií
29. Nasazení webového filtru v transparentním nebo netransparentním režimu pro http
30. Výjimky z HTTPS inspekce na určené zdrojové IP, servery nebo kategorie
31. Kontrola HTTPS provozu, ověřování certifikátu na proxy
32. Definice důvěryhodných CA, podpis nedůvěryhodných CA
33. Kategorizace webových domén dle obsahu v počtu min. 50ks, kategorizační databáze nezávislá na online službě nebo cloudu, databáze kategorií v rámci dodávky
34. Samostatné kategorie domén pro www se škodlivými kódy a P2P
35. Politika přístupu uživatele na služby definovaná dle času, kategorií, cílové adresy, uživatele, skupiny uživatelů
36. Definice vlastní kategorie serverů
37. Kategorizace webových stránek podle celé URL adresy
38. Ověřování přenášených souborů na základě MIME type i CONTENT type, nastavení pravidla pro zákaz přenosu
39. Detekování typů přenášených souborů v HTTP/HTTPS komunikaci
40. Definice black/white listů (uživatel, skupina, IP adresa)
41. Reklamace chybného záznamu pomocí webového formuláře, zpětná vazba, rychlost reakce na ruční hlášení do 48h v pracovní dny
42. Aktualizace webového filtru o nezařazené domény z webového provozu v pracovní dny do 48h
43. Interface pro protokol ICAP na zapojení externího antiviru (např. ClamAV)
44. Antivirové řešení pro kontrolu stahovaného obsahu přes webovou proxy
    1. skenování určených typů souborů
    2. skenování archivů, instalačních balíčku, OLE objektů
    3. blokování přístupu na infikovaný/podezřelý objekt, informování uživatele
    4. odstranění infekce (pokud to je možné)
    5. konfigurace reportů, logování událostí
45. Monitoring provozu, statistiky provozu, periodické reporty o provozu, údaje o úspěšné kategorizaci provozu přes filter (http i https), nástroj na prohledávání logů firewallu i webové proxy, log aktivity správce zařízení
46. Nastavení doby pro uchování záznamů na lokálním úložišti logů
47. Logování na externí server přes protokol Syslog (aktivita správce, firewall log, …)
48. Zachycení provozu pro následnou analýzu (dump provozu pro následnou analýzu např. ve Wiresharku)
49. Perpetual licenční pokrytí veškeré požadované funkcionality včetně maintenace dle rámcové smlouvy
50. Navýšení počtu uživatelů o 30% formou doplnění licencí - bez dalších změn HW a SW
51. Dokumentace řešení, zaškolení obsluhy v počtu 2 osob v rozsahu 4 hodiny
52. Záruční doba na HW na dle rámcové smlouvy (v případě volby HW appliance)

**Nepovinné požadavky (zohledněno při hodnocení):**

1. Omezení délky trvání spojení maximálním množstvím přenesených dat (není nutné u navázaných session)
2. Zapnutí informace pro uživatele o dekrypci v případě potřeby a interace uživatele o převzetí informace
3. Definice důvěryhodných CA, podpis nedůvěryhodných CA, rozlišení typu chyb (expirace certifikátu, chybná doména, slabý šifrovací klíč …), podmíněné zpřístupnění na omezenou dobu
4. Upozornění a blokování kategorií serverů, podmíněné zpřístupnění na omezenou dobu (upozornění pro správce i uživatele)

**Komodita 6 - Firewall a web filter pro 1000 souběžných uživatelů**

Technické zadání musí splňovat všechny požadavky pro komoditu 5, kromě bodu 1. Bod 1 zadávací dokumentace je nahrazen následujícím textem:

1. Rozhraní 10 x 1000BASE-T, virtuální appliance pro VMWare ESX nebo HyperV

**Komodita 7 - Centrální dohledový software pro Firewall a web filter**

1. Vzdálené Integrovatelné do centrálního konzole/dohledu
2. Zálohování konfigurace dohledovaných zařízení (lze realizovat i službou operačního systému)
3. centralizování informací z jednotlivých zařízení
4. dohledování stavu a výkonu jednotlivých zařízení (firewallů) - vyčítání informací o stavu  zařízení (verze firmware, výkonové parametry zatížení, celkové zdraví zařízení, ….  )
5. statistiky, reporting s retencí minimálně 180 dní, automatické odesílání definovaných reportů e-mailem
6. syslog, alerting administrátora (zaslání informace o změně stavu systému)
7. architektura klient – server, šifrované připojení klienta
8. licence pro dohled minimálně 20 zařízení a připojení současně přihlášených 5 klientů do systému
9. server musí být dodán jako virtuální appliance pro VMWare ESX nebo HyperV

##### Společné parametry platné pro komoditu 1 až 6

Nastavení veškerých požadovaných funkcí bude k dispozici přes CLI, v grafickém prostředí zařízení musí být dostupné minimálně tato nastavení:

1. Přehledný dashboard s informací o celkovém stavu zařízení včetně provozních výkonových parametrů, výstražná upozornění na chyby případně incidenty, informace o IP na interfaces,
2. Informace o spuštěných službách
3. Informace o směrovací tabulce
4. Seznam aktuálně přihlášených VPN uživatelů s možností ukončení session
5. Konfigurace kompletních FW pravidel včetně NAT
6. Konfigurace uživatelů VPN
7. Konfigurace vlastností uvedených v zadávací dokumentaci u webové proxy
8. Monitoring provozu – logy, reporty, statistiky
9. Konfigurace DHCP serveru včetně obsazenosti dynamických pool (pokud je požadován)
10. Restart zařízení, update firmware, záloha a obnova konfigurace

Řešení musí obsahovat potřebné časově neomezené licence vyplývající z výše uvedených požadavků a zařízení musí plnit všechny požadované funkce po dobu platnosti záručních a servisních podmínek ( viz rámcová smlouva).

##### Podmínky podpory výrobce platné pro všechny komodity

1. poskytnutí aktualizačních databází pro zakoupené aplikační filtry (webová proxy, antivirová databáze, …),
2. poskytnutí nových verzí firmware,
3. odstranění známých zranitelností firmware do 30 dnů od nahlášení vydáním nové verze,

**Akceptační testy pro všechny komodity (příloha č. 4 rámcové smlouvy)**

1. nastavení automatického přesměrování provozu klienta přes proxy bez zásahu uživatele do konfigurace koncového zařízení i pro případ mobilního přenosného zařízení (např. notebook)
2. nastavení a ukázka autentizace uživatelů webproxy oproti MS Active directory, LDAP, lokální databáze uživatelů (protokol Kerberos nebo NTLM) bez nutnosti instalace klientského SW na stanici
3. nastavení a ukázka konfigurace a provozu VPN pro zařízení s OS Windows, Linux, Android, iOS
4. nastavení a ukázka L7 aplikační kontroly (nebo zablokování) pro P2P sítě, sociální sítě
5. nastavení flow sběru dat a kontrola doručení dat (IP pro kolektor bude specifikována zadavatelem)
6. nastavení a ukázka kontroly HTTPS provozu – ověřování certifikátu na proxy, nastavení výjimek z inspekce
7. nastavení a ukázka kategorizace domén pro www – správa kategorizace, aktualizace, nastavení výjimek, definice vlastní kategorie
8. nastavení a ukázka politik pro uživatele – přístup na služby definované dle času, kategorií, cílové adresy, uživatele, skupiny uživatelů
9. nastavení a ukázka funkčnosti antivirového řešení