

University of Southeastern Philippines Bids and Awards Committee

BAC Resolution Declaring Lowest Calculated & Responsive Bidder (LCRB) and Recommending Award of Contract

RESOLUTION NO. 2020-06

WHEREAS, the University of Southeastern Philippines advertised the Invitation to Bid for the Procurement of ICT Equipment (Hardware & Software Services) for USeP-SDMD Obrero Campus, Davao City, with a budget allocation of Five Million Two Hundred Sixty Thousand Pesos (PhP 5,260,000.00) and posted the same in the PhilGePS on September 17 to 24, 2020, on the University website, and in conspicuous places like USeP Main Gate Bulletin Board on the same period;

WHEREAS, on 25 September 2020, the Bids and Awards Committee (BAC) held the prebid conference which were attended by two (2) bidders, namely: Columbia Computer Center & Trey-D Enterprises;

WHEREA, on 09 October 2020, the scheduled opening of bids, there were two (2) bidders submitted its bid proposal and passed the preliminary examination of bids namely: Columbia Computer Center and Unicenter Communications;

WHEREAS, the bid proposal of the two (2) eligible bidders were found to be substantially complying;

WHEREAS, the detailed bid evaluation and validation of the specifications was conducted by the TWG, while the bid evaluation was carried out by the BAC on 23 October 2020, that resulted in the following:

DESCRIPTION/SP ECIFICATIONS	UNIT COST	COLUMBIA CO CENTER (DAV		Findings	UNIC COMMU	Findings	
1. High Volume and Precision Document Scanner	50,000.0 0	Epson 780N Document Scanner	49, 600.00	complying	CANON DRC240	49, 500.00	Not complying
2. Android/Smart TV	50,000.0 0	HISENSE 50" SMART TV	38, 077.00	complying	SAMSUNG UHD	48, 500.00	
3. Photocopying Machine (for Legal, A4 up to A3 Document Format)	67, 500.00			NO BID	FUJI XEROX DOCUCENT RE S2320	64, 500.00	complying
4. 3 in 1 Wireless/Duplex with ADF Printer	16, 000.0			NO BID	EPSON L6170	15, 800.00	Not complying
5. Firewall (High Performance	3, 000, 000.00	FORTIGATE 1000D	2,615,061.	complying	SOPHOS XG550	2, 980, 000.	

WE BUILD DREAMS WITHOUT LIMITS

Address: University of Southeastern Philippines Iñigo St., Bo. Obrero, Davao City Philippines 8000



appliance based Firewall that facilitate multi- application environment, min. of 1, 000 concurrent users)							
6. Manageable Switch	51, 000.00	CISCO SG350-28P	38, 481.48	complying	CISCO SG350-28P	49, 500.00	
7. Access Point Router	15, 500.00	UBIQUITI UAP AC LR (UNIFI AC)	7, 800.00	complying	UBIQUITI UAP AC LR	14, 500.00	
8. Server	470, 000.00	HPE DL360 GEN10 8SFF CTO SERVER 4110	465, 500.00	complying	HPE DL360 GEN10 8SFF CTO SERVER 4214	468, 000.00	
9. Laptop	77, 000.00	ACER TRAVELMAT E TMP215 52G	58, 000.00	complying	HP NOTEBOOK 15S-DU203	38, 300.00	Not complying

WHEREAS, upon post-qualification or careful examination, validation and verification of all Eligibility, Technical and Financial documents submitted to the BAC by the bidder with the Lowest Calculated Bid (LCB), as presented in the Post-Qualification Evaluation Report, the Bidders namely: Columbia Computer Center for item numbers 1, 2, 5, 6,7, 8 & 9 and Unicenter Communications for item number three (3) with the Lowest Calculated and Responsive Bid (LCRB) and thus post-qualified for the items listed in Annex A, as attached to this Resolution;

NOW THEREFORE, We the Members of the Bids and Awards Committee. Hereby **RESOLVE**, as it is hereby **RESOLVED**:

- 1. To declare Columbia Computer Center, as the Bidder with the Lowest Calculated and Responsive Bid for item numbers 1, 2, 5, 6,7, 8 & 9;
- 2. To declare **Unicenter Communications**, as the Bidder with the Lowest Calculated and Responsive Bid for item number **three** (3);
- 3. To declare item number **four (4)** as **Rebid**, the two bidders are not compliant & to recommend the said item for Alternative Method of Procurement thru Shopping; and
- 4. To recommend to the Head of Procuring Entity for approval of the foregoing findings.

Telephone: (082) 227-8192 local 309

bac@usep.edu.ph

Website: www.usep.edu.ph

RESOLVED, at the University of Souhteastern Philippines, Obrero Campus, Davao City, Philippines, this _____ day of December 2020.





REYNALDO M. NOGODULA

BAC Vice Chair

JOSE ALTHER M. RIVERA BAC Member

RHINNA M. SAAN

BAC Alternate Member

RIOLIZA B. MOLINA BAC Member

NIMFA V. MANISCAN BAC Alternate member

APPROVED:

(Per BOR Resolution No. <u>144</u>20<u>1</u>9

RDES C. GENERALA

SUC President



Philippines 8000



Technical Specification Evaluation: (Columbia Computer Center & Unicenter Communications)

DESCRIPTION/SPECIFICATIONS	UNIT COST	COLUMBIA COMPU (DAVAO) INC.	TER CENTER		UNICENTER COMMUNICATIONS		
High Volume and Precision Document Scanner	50,000.00	Epson 780N Document Scanner	49, 600.00	FINDINGS	CANON DRC240	49, 500.00	FINDINGS
1. B&W / Grayscale / Color 2. Simplex / Duplex 3. 60- sheet capacity ADF 4. Up to 45ppm 5. Up to 600 dpi resolution 6. Up to A4 & Legal size 7. Duty Cycle:4,000 per day 8. Double feed detection 9. Advanced text enhancement 10. Skip blank page 11. Prescan 12. Auto paper detection 13. Deskew 14. Text orientation recognition 15. Folio scanning 16. CaptureOnTouch 17. CapturePerfect 18. Ethernet Connectivity		1. Complying 2. Complying 3. Complying 4. Complying 5. Complying 6. Complying 7. Complying 9. Complying 10. Complying 11. Complying 12. Complying 13. Complying 14. Complying 15. Complying 16. Complying 17. Complying 18. Complying		Items on red is for verification.	1. Complying 2. Complying 3. Complying 4. Complying 5. Complying 6. Complying 7. Complying 8. Complying 9. Complying 10. Complying 11. Complying 12. Complying 13. Complying 14. Complying 15. Complying 16. Complying 17. Complying 18. Not complying		Not complying.
2. Android/Smart TV	50,000.00	HISENSE 50" SMART TV	38, 077.00		SAMSUNG UHD	48, 500.00	
1. LED Smart TV 50" 2. Atleast 2 HDMI ports 3. Component connectivity 4. USB ports 5. Ethernet connectivity 6. Wifi capable 7. Wall Mount 3. Photocopying Machine (for Legal, A4 up to A3 Document Format) 1. Heavy Duty Photocopier Machine 2. Copier, Printer, Scanner; 3. Copy speed of at least 22 copies per minute for A4 4. Paper size up to A3 5. Continuous copying up to 999 6. Zoom range 25 to at least 400% 7. With document processor, interrupt copy function, electronic sort function 4. 3 in 1 Wireless/Duplex with ADF	67, 500.00	Complying Complying Complying Complying Complying Complying Complying complying complying	NO BID	Items on red is for verification.	FUJI XEROX DOCUCENTRE S2320 1. Complying 2. Complying 3. Complying (max. paper size 297 x 432 mm) 5. Complying 6. Complying	64, 500.00	
Printer 1. Print, Scan, Copy, Fax with ADF 2. With at least having the following specifications: 4,800 x 2,400 dpi resolution. 3. 2.8 pl ink droplet volume 4. Print speed for draft text 32 ppm/20 ppm and photo 42 sec per photo			NO BID		Complying Not Complying (4800 x 1200 dpi) Not Complying (3.3 pl) Complying		Non Complying

WE BUILD DREAMS WITHOUT LIMITS

Address: University of Southeastern Philippines Iñigo St., Bo. Obrero, Davao City

Philippines 8000



	5.	Automatic 2 sided printing							
	6.	B&W and Colored A4 copy							
		speed 16 ipm/8.8 ipm							
	٦,								
	7.	Copy resolution 600 x 600							
		dpi					Complying		
	8.	Scan area 297.18 x 431.8					6. Not		
		mm					Complying		
	9.	ADF support 64-95 g/m2 at					7. Not		
	9.								
		least 35 pages capacity					Complying		
	10.	Support paper size A3+,							
		A3, A4, A5, A6, B4, B5,							
		Legal, Letter, Half Letter, 5							
		x 7 ", 4 x 6 ", 3.5 x 5 " and							
		329 x 1200 mm							
	11.	3 paper trays at least 250							
		sheets capacity A4 plain							
		paper 80 g/m2 20 sheets							
		premium glossy photo							
		paper							
	12	Ethernet Wi-Fi IEEE							
	12.								
		802.11 b/g/n, Wi-Fi Direct,							
		and USB interfaces.							
5.	Firew	all (High Performance	3, 000,	FORTIGATE 1000D	2,615,061.		SOPHOS	2, 980, 000.	
		ce based Firewall that	000.00		,		XG550		
		multi-application	220.00						
		ment, min. of 1, 000							
СО	ncurr	ent users)							
	1.	High Availability and							
		scalable							
	2.	Rackmount Type							
	3.	Bundled Unified Software							
		(threat protection-IPS,							
		AMP, Web Filtering,							
		Antispam, etc.) for at least							
		1 year subscription							
		license							
	4.	Provide a HTTP, HTTPS,							
		SSH, Telnet, SNMP based							
		management console							
	_ ا								
	5.	Shall be in the Leaders'							
		Quadrant of Gartner Magic							
		Quadrant for the last 5							
		consecutive years							
	6								
	6.	Support ICSA and							
		compliance certifications]			
	7.	Capable of clustering]			
		multiple NGFWs together				1			
		into a redundant and highly							
		available stateful							
		configuration without extra							
		license cost				1			
	8.	Support LACP to achieve							
	٠			i					
							I	1	I
	0	higher bandwidth							
	9.	higher bandwidth Support WAN load balance							
		higher bandwidth Support WAN load balance Shall support Dynamic							
		higher bandwidth Support WAN load balance Shall support Dynamic							
		higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1							
		higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3,							
	10.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS							
	10.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy							
	10.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS							
	10.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast							
	10.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing							
	10.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party							
	10.11.12.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party authentication servers							
	10.11.12.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party authentication servers Support recommended SD							
	10.11.12.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party authentication servers							
	10.11.12.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party authentication servers Support recommended SD WAN rules by parties such							
	10.11.12.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party authentication servers Support recommended SD WAN rules by parties such as NSS Labs, support							
	10.11.12.	higher bandwidth Support WAN load balance Shall support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS Support Static, Policy Based, and Multicast routing Shall support 3rd party authentication servers Support recommended SD WAN rules by parties such							



Transparent 14. Support Central NAT 16. Ready for Sandboung integration either doubt or cor premise and even the filtering must be available to all policies 17. Support per policy SSL/SSH decryption & inspection 18. Support SSL orithant inspection 29. Support SSL orithant inspection 20. Support SSL orithant inspection 20. Support SSL orithant inspection 21. Support affects sharing 21. Support network relatic classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Compty-support industry standards in RSC, and SSL softemal solution, hardware or modulas 24. Must have builten hardware VPN acceleration to support IPSEC (DES, 3DES, RSES) anchyptonidecryption, SSL encryptonidecryption, SSL encryptonidecryption, SSL encryptonidecryption, support indust 28. Support MSG of SSL Supports NAT Traversal 29. Support Nat Traversal 29. Support Nat Traversal 29. Support Hub and Spoke architecture 20. Supports Nat Traversal 29. Supports Hub and Spoke architecture 29. Support at least 5 Caps Fireval Throughput 29. Support at least 5 Caps Fireval Throughput 39. Support at least 6 Caps Fireval Throughput 49. Support at least 6 Caps Fireval Throughput 40. Support at least 6 Caps Fireval Throughput	 	- 1		ı		
15. Ready for Sandboxing Integration either claud or on premise 16. Anthrous, antispam, ips, and web filtering must be available to all prolices 17. Support for polity in S.S.L.SST decryption 8. Support St. officiality in Support St. off	11					
Integration either cloud or on premise 16. Antorius, antispani, jps, and velo filtering must be available to all policies 17. Support of profices 18. Support SSL content 19. Support SSL content 20. Support OSP bollop-based/raffic shaping 21. Support oSP bollop-based/raffic shaping 22. Support network traffic dashifted in the profit of the special content of the application without service restart or reboot requirement of the application without service restart or reboot requirement of the special content of the spec						
on premise 16. Anthritis, anthopen, lps, and web filtering must be available to all policios 17. Support per policy SSLISH decyption & inspection 18. Support SSL dindering 19. Support SSL dindering 19. Support SSL dindering 19. Support network traffic dissification 24. Allow dynamic updates of the application without service restant or reboot requirement 26. Comphysipport industry standards PSEC, and SSL actional solution, and any action or modules 27. Many these built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, supports Policy and Route base VPN 25. Support MDS or SHA 1 authentication and data Authentication 28. Supports NAT Traversal 27. Support SAT Taversal 27. Support SAT Taversal 28. Supports VAL Taversal 29. Supports VAL Taversal 29. Supports VAL Taversal 21. Support IPSEC (DES, 3DES, AES) encryption-februphic properts in the support of the support Note VPN 30. Support MDS or SHA 1 authentication 30. Supports VAL Taversal 31. Support AUT Taversal 32. Support SAT Taversal 33. Support at least 5 Cipps Firewall Throughput 34. Support at least 6 Cipps Firewall Throughput 35. Support at least 6 Cipps Firewall Throughput 36. Support at least 6 Cipps Firewall Throughput 37. Support at least 6 Cipps Firewall Throughput 38. Support at least 6 Cipps Firewall Throughput 39. Support at least 6 Cipps Firewall Took hardware Accelerated 1 Cic SEP- Siols Siols	15.					
16. Antivirus, antisparm, jus, and web filtering must be available to all policilos (7). Support per policity (7). SUSSH decryption & inspection (8). Support SSL ortheating (9). Support selection (9). Support SSL selection (9). Support SSL selection (9). Support MSD or SHA 1 authentication and data integrity (9). Support MSD or SHA 1 authentication and data integrity (9). Support SSL sensible LANGVOLD (9). Support Standard Authantication and data integrity (9). Support Standard Authantication (9). Supports Standard Authantication (9). Supports Standard (9). Support states Standard (9). Support						
and web filtering must be available to all policies 17. Support per policy SSLSSH decryption & inspection 18. Support SSL offloading 19. Support SSL offloading 19. Support SSL offloading 19. Support SSL offloading 20. Support CSS Policy- based/Taffic shaping 21. Support network traffic Cassification updates of cassification updates of the application without senior restant or reboot requirement 22. Comply/support industry standards IPSCC, and SSL VPN without additional external solution, hardware or modules 24. Must have bull-in hardware vPN acceleration to support IPSCC (DES, 3DES, AES) ancrypton/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MDS or SH 1 authentication and data integrity 27. Authentication and data integrity 28. Support MD and Spube acceleration to support Section of the support Section of the support Section of the support Section of the support MDS or SH 1 authentication and data integrity 27. Support MDS or SH 1 authentication and data integrity 28. Support MD and Spube architecture 29. Support Section of the support Section of the support of the Section of the support	16					
available to all ploiloise 17. Support per policy \$SL/SSH decryption & inspection 18. Support SSL ordinating 19. Support SSL content inspection 20. Support DSS Policy-based/Traffic shaping 21. Support network traffic classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Complysupport industry standards in SEC, and SSL VPN without additional external solution, hardware of the supplication without additional external solution, hardware of the supplication without additional external solution, hardware of the support IPSEC (DES, 30ES, AES) 24. Must have built-in landware VPN acceleration in support IPSEC (DES, 30ES, AES) 25. Encryption/decryption, SSL encryption	10.					
17. Support per policy SSLSSH decryption & inspection 18. Support SSL ordinating 19. Support SSL ordinating 19. Support SSL ordinating 20. Support CSS Policy- based Traffic shaping 21. Support network staffic classification 22. Allow dynamic update of the application without sense the control of the application of the application without sense the control of the application of the						
SSL/SSH decryption & inspection 18. Support SSL dinading 19. Support SSL cinetent inspection 20. Support DSL content inspection 21. Support on the work fraffic classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardward over the content of the set of t	17					
inspection 18. Support SSL difloading 19. Support SSL content inspection 20. Support CoS Policy- based/Traffic shaping 21. Support network traffic dassification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 30ES, AES) encyption/decyption, supports Policy and Route base VPN 25. Support MSO or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Author Traversal 28. Supports Hut and Spoke architecture 29. Supports Hut and Spoke architecture 31. Supports situal Extensible Journal of Supports Studie Extensible Journal of Supports Studie Extensible Journal of Supports I and Traversal 28. Support situal Extensible Journal of Spoke architecture 31. Support alloads 15 Cbps Fineal Introughput 32. Support alloads 15 Cbps Fineal Introughput 33. Support alloads 15 Cbps Fineal Introughput 34. Support alloads 15 Cbps Fineal Introughput 35. Support alloads 15 Cbps Fineal Introughput 36. Support alloads 15 Cbps Fineal Introughput 37. Support alloads 15 Cbps Fineal Introughput 38. Support alloads 15 Cbps Fineal Introughput 39. Support alloads 15 Cbps Fineal Protection Throughput 30. Support alloads 15 Cbps	17.					
18. Support SSL content inspection 29. Support Oss Policy-based/Traffic shaping 21. Support network traffic classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3) DES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MSD or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports NAT Traversal 27. Supports NAT Traversal 28. Supports NAT Traversal 29. Support situal Extensible LAN (NXLAN) 30. Support at least 5C Obps Firewall Throughput 31. Support at least 5C Obps Firewall Throughput 32. Support at least 5C Obps Infraversal Provincion Throughput 31. Support at least 5C Obps Infraversal Support 2x Hardware Accelerated 10 CE SPP Siots 33. Support 2x Hardware Accelerated 10 CE SPP Siots						
19. Support SSL content inspection 20. Support CoS Policy-based/Traffic shaping 21. Support network traffic classfication 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Comply/support industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, supports POlicy and Route base VPN 25. Support NDS or SHA 1 authentication and data intendication and data intendication and data intendication and data intendication and data schemication and data schemication and data schemication and data schemication and spoke architecture 29. Supports NAT Traversal 27. Supports NAT and Traversal 29. Supports situal Extensible La (VC NAW) 30. Supports situal Extensible La (VC NAW) 31. Support al least 5 C Sps Firewall Throughput 32. Support al least 15 C Sps Firewall Throughput 33. Support al least 15 Cops NSFW Throughput 34. Support al least 15 Cops NSFW Throughput 35. Support al least 15 Cops NSFW Throughput 36. Support al least 15 Cops NSFW Throughput 37. Support al least 15 Cops NSFW Throughput 38. Support al least 15 Cops NSFW Throughput 39. Support al least 15 Cops NSFW Thro	10					
inspection 20. Support Qos Policy-based/Traffic shaping 21. Support network traffic classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have buill-in hardware VPN accoleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA1 sutherincation and data integrity 26. Supports NAT Traversal 27. Supports And Autherication 28. Supports Hub and Spoke architecture 29. Supports Hub and Spoke architecture 29. Support situate Extensible LAN (YXLAN) 30. Support at least 52 Gbps Firewall Throughput 31. Support at least 15 Gbps Firewall Throughput 32. Support at least 15 Gbps Firewall Throughput 33. Support at least 15 Gbps In Firewall Support at least 15 Gbps In Firewalls 34. Support at least 15 Gbps In Firewalls 35. Support at least 15 Gbps In Firewalls 36. Support at least 15 Gbps In Firewalls 37. Support at least 15 Gbps In Firewalls 38. Support at least 15 Gbps In Firewalls 39. Support at least 15 Gbps In Firewalls 31. Support at least 15 Gbps In Firewalls 32. Support at least 15 Gbps In Firewalls 33. Support at least 15 Gbps In Firewalls 34. Support at least 15 Gbps In Firewalls 35. Support at least 15 Gbps In Firewalls 36. Support at least 15 Gbps In Firewalls 37. Support at least 15 Gbps In Firewalls 38. Support at least 15 Gbps In Firewalls 39. Support at least 15 Gbps In Firewalls 39. Support at least 15 Gbps In Firewalls 39. Support at least 15 Gbps In Firewalls 30. Support at least 15 Gbps In Firewalls 31. Support at least 15 Gbps In Firewalls 39. Support at least 15 Gbps In Firewalls 39. Support at least 15 Gbps In Firewall In Fir						
20. Support CoS Policy-basedTraffic Shaping 21. Support network traffic classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. ComplySupport industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryptio	19.					
2.1 Support network treffic dassification 2.2 Allow dynamic updates of the application without service mistart or reboot requirement 2.2 Camply/support industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 4.4 Must have built-in hardware VPN acceleration to support IPSEC (DES, 30ES, AES) 9.1 encryptionidecryption, SSL encryptionidecryption, SSL encryptionidecryption, SSL encryptionidecryption, supports Policy and Route base VPN 2.5 Support MIDS or SHA 1 authentication and data integrity 2.6 Supports MST Travesal 2.7 Supports Extended Authentication and Spoke architecture 2.8 Supports Hub and Spoke architecture 2.9 Supports withat Extensible LAN (VXLAN) 3.0 Support with a Extensible LAN (VXLAN) 3.0 Support at least 52 Clabs Firewall Throughput 3.1 Support at least 64 Clabs Application Control Throughput 3.2 Support at least 65 Clabs Firewall Throughput 3.3 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support at least 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support 16 Clabs 65 Clabs Interval 10 Clabs Application Control Throughput 3.5 Support 16 Clabs 65 Clabs Interval 10 Clabs 65	20	Support OoS Policy				
22. Allow dynamic updates of the application without service restart or reboot requirement and an advanced by the application without service restart or reboot requirement as the application without additional external southon, hardware or modules at the acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SL encryption/decryption/decryption/decryption/decryption, SL encryption/decryption, SL encryption/decryp	20.					
classification 22. Allow dynamic updates of the application without service restart or reboot requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 30ES, AES) encryptionidecryption, SSL encryptionidecryption, SSL encryptionidecryption, SSL encryptionidecryption, supports Policy and Route base VPN 25. Support MISF or SHA 1 authentication and data integrity 26. Supports MST Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (YXLAN) 30. Support with a Extensible LAN (YXLAN) 31. Support at least 52 Cbps Firewall Throughput 32. Support at least 10 Virtual Firewalls 43. Support at least 6 Cbps NGFW Throughput 33. Support at least 6 Cbps NGFW Throughput 34. Support at least 6 Cbps NGFW Throughput 35. Support at least 6 Cbps NGFW Throughput 36. Support at least 6 Cbps NGFW Throughput 37. Support at least 6 Cbps NGFW Throughput 38. Support at least 6 Cbps NGFW Throughput 39. Support at least 6 Cbps NGFW Throughput 49. Support at least 6 Cbps NGFW Throughput 49. Support at least 6 Cbps NGFW Throughput 49. Support at least 6 Cbps NGF	21					
22. Allow dynamic updates of the application without service restart or reboot requirement 23. Comply/support industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware vPN acceleration to support IPSEC (DES, 3DES, AES) encyption/decryption, SL encryption/decryption, supports Policy and Route base VPN 25. Support MDS or SHA1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication and data integrity 28. Supports Hub and Spoke architecture 29. Supports Wat al Extensible LAN (VXLAN) 30. Support web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 16 Gbps IPS Throughput 35. Support at least 16 Gbps IPS Throughput 36. Support at least 16 Gbps IPS Throughput 37. Support at least 16 Gbps IPS Throughput 38. Support at least 16 Gbps IPS Throughput 39. Support at least 16 Gbps IPS Throughput 31. Support at least 6 Gbps IPS Throughput 32. Support at least 6 Gbps IPS Throughput 33. Support at least 6 Gbps IPS Throughput 34. Support at least 6 Gbps IPS Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support 24 Hardware Accelerated 10 GE SFP- Slots	۷١.					
the application without service restait or reboot requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardware external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MDS or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Extended E	22					
service restart or reboot requirement 23. Comply/support industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 30ES, AES) encyption/decryption, SSL encyption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports NAT Traversal 27. Supports Nat Descended Authentication 28. Supports Wat and Extensible LAN (VX.AN) 30. Support wirtual Extensible LAN (VX.AN) 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 14 Gbps Application Control Throughput 34. Support at least 15 Gbps I Firewall Shapping Shap	22.					
requirement 23. Complysupport industry standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MDS or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports SAT Traversal 27. Supports SAT traversal 28. Supports SAT traversal 29. Supports SAT Traversal 30. Supports SAT Standard Authentication 40. Supports SAT Standard Authentication 40. Supports SAT Standard S						
23. Comply/support industry standards IPSEC, and SLS VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 30ES, AES) encryption/decryption, SLS, encryption/decryption, supports Policy and Route base VPN 25. Support MDS or SHA 1 authentication and data integrity 26. Supports Nat Traversal 27. Supports Extended Authentication and adda rarchitecture 29. Supports Virtual Extensible LAN (VXLAN) 30. Support without Extensible LAN (VXLAN) 31. Support at least 12 Gbps Application Control Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Friewalls 34. Support at least 10 Virtual Friewalls 35. Support at least 10 Virtual Friewalls 36. Support at least 10 Virtual Friewalls 37. Support at least 10 Virtual Friewalls 38. Support at least 10 Virtual Friewalls 39. Support at least 10 Virtual Friewalls 31. Support at least 10 Virtual Friewalls 32. Support at least 10 Virtual Friewalls 33. Support at least 10 Virtual Friewalls 34. Support at least 10 Virtual Friewalls 35. Support at least 10 Virtual Friewalls 36. Support at least 10 Virtual Friewalls 37. Support 27. Hardware Accelerated 10 GE SFP+ Slots Slots						
standards IPSEC, and SSL VPN without additional external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encyption/decryption, SSL encyption/decryption/decryption/decryption/decryption/decryption/decryption/decryption/decryption/decryption/decryption/decryption/d	23					
VPN without additional external solution, hardware or modules 24. Must have built-in hardware vPN acceleration to support IPSEC (DES, 3)DES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports Extended Authentication and solve architecture 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports witual Extensible LAN (VXLAN) 30. Support witual Extensible LAN (VXLAN) 31. Support at least 12 Cbps Firewall Throughput 32. Support at least 14 Cbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Cbps NGFW Throughput 35. Support at least 6 Cbps IPS Throughput 36. Support at least 6 Cbps IPS Throughput 37. Support 2x Hardware Accelerated 10 CE SFP Slots 38. Support 16x Hardware Accelerated 10 CE SFP Slots	20.					
external solution, hardware or modules 24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support Mbo or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Evended Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support wirtual Extensible LAN (VXLAN) 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 14 Orbitual Firewalls 34. Support at least 15 Gbps NGFW Throughput 35. Support at least 16 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support at least 6 Gbps IPS Throughput 38. Support at least 6 Gbps IPS Throughput 39. Support at least 6 Gbps IPS Throughput 30. Support at least 6 Gbps IPS Throughput 31. Support at least 6 Gbps IPS Throughput 32. Support at least 6 Gbps IPS Throughput 33. Support at least 6 Gbps IPS Throughput 34. Support at least 6 Gbps IPS Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support 24 Hardware Accelerated 10 GE SFP+ Siots Slots						
or modules 24. Must have built-in hardware VPN acceleration to support PSEC (DES, 30ES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports Extended Authentication 27. Supports Extended Authentication 28. Supports Extended Authentication 29. Supports Hub and Spoke architecture 29. Support alteast Set Set Set Set Set Set Set Set Set Se						
24. Must have built-in hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Steinded Authentication 28. Supports thub and Spoke architecture 29. Support svirtual Extensible LAN (VXLAN) 30. Support at least 52 Gbps Firewall Throughput 31. Support at least 14 Gbps Application Control Throughput 33. Support at least 14 Gbps Application Control Throughput 33. Support at least 6 Gbps IPS Throughput 34. Support at least 6 Gbps IPS Throughput 35. Support at least 6 Gbps IPS Threat Part Aughentication Throughput 36. Support at least 6 Gbps IPS Threat Part Aughentication Throughput 37. Support at least 6 Gbps IPS Threat Part Aughentication Throughput 38. Support at least 6 Gbps IPS Threat Part Aughentication Throughput 39. Support at Aughentication Throughput 31. Support at Aughentication Throughput 32. Support at Aughentication Throughput 33. Support at Aughentication Throughput 34. Support at Aughentication Throughput 35. Support at Aughentication Throughput 36. Support at Aughentication Throughput 37. Support at Aughentication Throughput 38. Support at Aughentication Throughput 39. Support at Aughentication Throughput 31. Support at Aughentication Throughput 32. Support at Aughentication Throughput 33. Support at Aughentication Throughput 34. Support at Aughentication Throughput 35. Support at Aughentication Throughput 36. Support at Aughentication Throughput 37. Support at Aughentication Throughput 38. Support at Aughentication Throughput 39. Support at Aughenticatio						
hardware VPN acceleration to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports Extended Authentication 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports Witual Extensible LAN (VXLAN) 30. Support at least 52 Gbps Firewall Throughput 31. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls Firewalls 34. Support at least 10 Virtual Firewalls 35. Support at least 6 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support at least 6 Gbps IPS Throughput 38. Support at least 10 Virtual Firewalls 39. Support at least 10 Virtual Firewalls 31. Support at least 10 Virtual Firewalls 32. Support at least 10 Virtual Firewalls 33. Support at least 10 Virtual Firewalls 34. Support at least 10 Virtual Firewalls 35. Support at least 10 Virtual Firewalls 36. Support at least 10 Virtual Firewalls 37. Support at least 10 Virtual Firewalls 38. Support 16x Hardware Accelerated 10 GE SFP- Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	24					
to support IPSEC (DES, 3DES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports Extended Authentication 28. Supports Extended Authentication 29. Supports Hub and Spoke architecture 29. Supports witual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 44. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Cbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 5 Gbps IPS Throughput 39. Support at least 6 Cbps IPS Throughput 31. Support at least 6 Cbps IPS Throughput 32. Support at least 6 Cbps IPS Throughput 33. Support at least 6 Cbps IPS Throughput 34. Support at least 6 Cbps IPS Throughput 35. Support at least 6 Cbps IPS Throughput 36. Support at least 6 Cbps IPS Throughput 37. Support at least 6 Cbps IPS Throughput 38. Support at least 6 Cbps IPS Throughput 39. Support at least 6 Cbps IPS Throughput 31. Support at least 6 Cbps IPS Throughput 32. Support at least 6 Cbps IPS Throughput 33. Support at least 6 Cbps IPS Throughput 34. Support at least 6 Cbps IPS Throughput 35. Support at least 6 Cbps IPS Throughput 36. Support at least 6 Cbps IPS Throughput 37. Support at least 6 Cbps IPS Throughput 38. Support at least 6 Cbps IPS Throughput 39. Support at least 6 Cbps IPS						
and SDES, AES) encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports witual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 6 Gbps IPS Throughput 35. Support at least 4 Cbps NGFW Throughput 36. Support at least 4 Cbps Threat Protection Throughput 37. Support at least 4 Cbps Threat Protection Throughput 38. Support at least 6 Gbps IPS Throughput 39. Support at least 6 Cbps IPS Throughput 31. Support at least 6 Cbps IPS Throughput 32. Support at least 6 Cbps IPS Throughput 33. Support at least 6 Cbps IPS Throughput 34. Support at least 6 Cbps IPS Throughput 35. Support at least 6 Cbps IPS Throughput 36. Support at least 6 Cbps IPS Throughput 37. Support at least 6 Cbps IPS Throughput 38. Support at least 6 Cbps IPS Throughput 39. Support at least 6 Cbps IPS Throughput 30. Support at least 6 Cbps IPS Throughput 39. Support 20. Suppor						
encryption/decryption, SSL encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports witual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support all east 52 Gbps Firewall Throughput 32. Support all east 14 Gbps Application Control Throughput 33. Support all east 50 Gbps NGFW Throughput 34. Support at least 4 Gbps NGFW Throughput 35. Support at least 4 Gbps NGFW Throughput 36. Support at least 4 Gbps IPS Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps NGFW Throughput 39. Support at least 4 Gbps Throughput 31. Support at least 6 Gbps IPS Throughput 32. Support at least 4 Gbps Threat Protection Throughput 33. Support at least 4 Gbps Threat Protection Throughput 34. Support at least 4 Gbps Threat Protection Throughput 35. Support At least 5 Gbps NGFW Throughput 36. Support 4 Extraver Accelerated 10 GE SFP Slots						
encryption/decryption, supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 52 Gbps Firewall Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 4 Gbps NGFW Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support 2x Hardware Accelerated 10 GE SFP Slots						
supports Policy and Route base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports Virual Extensible LAN (VXLAN) 30. Support wive and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Throughput 37. Support at least 4 Gbps Throughput 38. Support at least 6 Gbps IPS Throughput 39. Support at least 6 Gbps IPS Throughput 31. Support at least 6 Gbps IPS Throughput 32. Support at least 6 Gbps IPS Throughput 33. Support at least 6 Gbps IPS Throughput 34. Support at least 6 Gbps IPS Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 10 GE SFP- Slots						
base VPN 25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports but and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 10 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 31. Support at least 4 Gbps Threat Protection Throughput 32. Support at least 4 Gbps Threat Protection Throughput 33. Support at least 4 Gbps Threat Protection Throughput 34. Support at least 4 Gbps Threat Protection Throughput 35. Support at Rardware Accelerated 10 GE SFP+ Slots Slots						
25. Support MD5 or SHA 1 authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 5 Gbps NGFW Throughput 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Cbps IFIEWAIL FIREWAIL FIREWAIL FIREWAIL Support at least 6 Gbps IFIEM Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 31. Support at least 4 Gbps Threat Protection Throughput 32. Support at least 4 Gbps Threat Protection Throughput 33. Support at least 4 Gbps Threat Protection Throughput Th						
authentication and data integrity 26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 50 Gbps NGFW Throughput 35. Support at least 6 Gbps PS Throughput 36. Support at least 4 Gbps Throughput 37. Support at least 4 Gbps Throughput 38. Support at least 4 Gbps Throughput 39. Support at least 4 Gbps Throughput 31. Support at least 5 Gbps Throughput 32. Support at least 6 Gbps PS Throughput 33. Support at least 6 Gbps Throughput 34. Support at least 6 Gbps PS Throughput 35. Support at least 6 Gbps Throughput 36. Support at least 6 Gbps Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	25.					
26. Supports NAT Traversal 27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 31. Support at least 4 Gbps Threat Protection Throughput 31. Support at least 4 Gbps Threat Protection Throughput 32. Support at least 4 Gbps Threat Protection Throughput 33. Support at least 4 Gbps Threat Protection Throughput 34. Support at least 4 Gbps Threat Protection Throughput 35. Support at least 4 Gbps Threat Protection Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots		authentication and data				
27. Supports Extended Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 10 Virtual Firewalls 35. Support at least 6 Gbps NGFW Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support at least 6 Gbps Threat Protection Throughput 38. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 31. Support at least 6 Gbps Threat Protection Throughput 32. Support at least 6 Gbps Threat Protection Throughput 33. Support at least 6 Gbps Threat Protection Throughput 34. Support at least 6 Gbps Threat Protection Throughput 35. Support at least 6 Gbps Threat Protection Throughput 36. Support at least 6 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 1 GE SFP+ Slots Slots		integrity				
Authentication 28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 31. Support 2x Hardware Accelerated 10 GE SFP+ Slots 32. Support 16x Hardware Accelerated 1 GE SFP Slots	26.	Supports NAT Traversal				
28. Supports Hub and Spoke architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Cbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 6 Gbps IPS Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 31. Support at least 4 Gbps Threat Protection Throughput 32. Support at least 4 Gbps Threat Protection Throughput 33. Support at least 4 Gbps Threat Protection Throughput 34. Support at least 4 Gbps Threat Protection Throughput 35. Support at least 4 Gbps Threat Protection Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Threat Prote	27.	Supports Extended				
architecture 29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 31. Support at least 4 Gbps Threat Protection Throughput 32. Support at least 4 Gbps Threat Protection Throughput 33. Support at least 4 Gbps Threat Protection Throughput 34. Support at least 4 Gbps Threat Protection Throughput 35. Support at least 4 Gbps Threat Protection Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 4 Gbps Threat Protection Throughput 38. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 4 Gbps Threat Protection Throughput 39. Support at least 5 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 6 Gbps Threat Protection Throughput 39. Support at least 10 Virtual Threat Protection Throughput 39. Support at least 10 Virtual Threat Protection Throughput 39. Support at least 10 Virtual Threat Protection Threat Protec						
29. Supports virtual Extensible LAN (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	28.	Supports Hub and Spoke				
LAÑ (VXLAN) 30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support at least 9 Gbps Threat Protection Throughput 38. Support 16 Kardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots						
30. Support Web and Tunnel Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	29.					
Mode VPN 31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots						
31. Support at least 52 Gbps Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	30.					
Firewall Throughput 32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	٠.					
32. Support at least 14 Gbps Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	31.					
Application Control Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	20					
Throughput 33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	32 .					
33. Support at least 10 Virtual Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots						
Firewalls 34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	33	Cupport at least 10 Vietual				
34. Support at least 5 Gbps NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	JJ.					
NGFW Throughput 35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	3/1					
35. Support at least 6 Gbps IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	υ 1 .	NGFW Throughout				
IPS Throughput 36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	35					
36. Support at least 4 Gbps Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	JJ.					
Threat Protection Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	36					
Throughput 37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	55.					
37. Support 2x Hardware Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots						
Accelerated 10 GE SFP+ Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots	37					
Slots 38. Support 16x Hardware Accelerated 1 GE SFP Slots						
38. Support 16x Hardware Accelerated 1 GE SFP Slots						
Accelerated 1 GE SFP Slots	38.					
Slots						
		Slots				
39. Support 16x Hardware	39.	Support 16x Hardware				



						Γ	T	1	
		Accelerated GE RJ45							
	40	Ports							
	40.	Support 1x 256 GB SSD							
	11	onboard storage Support Redundant Power							
	41.	Support Redundant Power Supply							
	12	256 GB SSD Onboard							
	42.	Storage,							
	43	16 Hardware Accelerated							
	FU.	GE RJ 45 ports, 2 GE							
		RJ45 management/HA							
		ports,							
	44.	USB ports,							
		Hardware accelerated 10							
		GE SFP+Slots,							
	46.	Hardware accelerated GE							
		SFP Slots,							
		6 Gbps IPS Throughput,							
	48.	4 Gbps Threat Protection							
	40	Throughput,							
	49.	3 microsecond Firewall							
	50	Latency (UDP, 64 bytes), Mpps Firewall Throughput,							
		11 Million Concurrent							
	J1.	Sessions (TCP),							
	52	100,000 Firewall Policies,							
		3.6 Gbps SSL-VPN							
		Throughput,							
	54.	5 Gbps SSL Inspection							
		Throughput,							
	55.	800,000 SSL Inspection							
		Concurrent Sessions,							
	56.	14 Gbps Application							
	F7	Control Throughput							
	57.	Active-active high							
	52	availability configuration, Active-Passive high							
	50.	availability configuration,							
	59.	Clustering high availability							
		configuration,							
	60.	Rack Mount, 100-240V							
		AC,							
	61.								
	00	Supply,							
	62.	Hot swappable redundant							
	62	power supply. Include installation up to							
	03.	latest security update,							
		deployment, post							
		installation evaluation and							
		validation, testing,							
		configuration summary							
		documentation, knowledge							
		transfer through technical							
	<u> </u>	training.	-4					44	
6.1	Manag	geable Switch	51, 000.00	CISCO SG350-28P	38, 481.48		CISCO SG350-	49, 500.00	
-	1	Lover 2 Dest Cischit		1 Complian		Compleins	28P		
	1.	Layer 3 Port Gigabit PoE+Managed Switch ,		 Complying Complying 		Complying			
	2.	28 Ports		z. Compiying					
7. /		ss Point Router	15, 500.00	UBIQUITI UAP AC	7, 800.00		UBIQUITI UAP	14, 500.00	
'''		Olin Noutel	10, 000.00	LR (UNIFI AC)	., 000.00		AC LR	1-7, 000.00	
	1.	AP, AC Long Range		1. Complying		Complying			
		Wireless Access Point;		2. Complying		1,5			
	2.	Preferably: Ubiquiti, Unifi		. , 0					
		for system compatability							
8. \$	Serve	r	470,	HPE DL360 GEN10	465,		HPE DL360	468,	



		000.00	8SFF CTO SERVER 4110	500.00		GEN10 8SFF CTO SERVER 4214	000.00	
	 Form Factor: 1U rack Processor: Generation: Gen10; Frequency: 3.0 GHz; Cores: 12; Power: 150W; Speed: 2666MT/s;L3 Cache: 24.75MB RAM: 128 GB (32 GB x 4 RDIMM DDR4 (Dual Rar 2666MT/s Storage: 1.2 TB (4 x 300 GB) SAS 12G Enterprise 15K SFF Hard Disk Drive Form Factor: 2.5 inch Power Supply: 2 x 500W Flex Slot Platinum Hot P Low Halogen Optical Drive: 9.5mm SATA DVD-RW G9 Optic Drive Others: Display Port/USB/Optical Drive Blank Kit, Sliding Rails With Cable Management Arm 	k) ; ug al	 Complying Complying Complying Complying Complying Complying Complying Complying Complying 		Items on red is for verification. The model offered is capable for such specificatio n. Need absolute specificatio n on the items on red text.			
9. L	Laptop	77, 000.00	ACER TRAVELMATE TMP215 52G	58, 000.00		HP NOTEBOOK 15S-DU203	38, 300.00	
	 Processor: 8th Generatin Dual Core 1.8 GHz Base Frequency, 4.6 GHz Turk Frequency, 8MB L2 Cacles; Graphics: Integrated UHI Graphics; Display: 15.6-inch LED-backlit FHD (1920 x 1080 anti-glare; Memory: 16GB DDR4 RAM; Storage: 512 GB PCIe SSD; Camera: HD Infrared webcam; Connectivity: Dual-band 802.11 ac compatible Wi Fi, Bluetooth Wireless 5. technology; I/O Ports: 1 x USB 3.1 G2 Type-C, 1 x USB 3.1 Type-A, 1 x USB 3.0 Type A, 1 x Standard HDMI, 1 SD Card Reader; OS: 64-bit OS, Window 10 Pro 	one)) en en en en en en	1. Complying 2. Complying 3. Complying 4. Complying 5. Complying 6. Complying 7. Complying 9. Complying 9. Complying			1. Not Complying (Base Freq: 1.0 Ghz)		Not Complying

