ANEXO 7

TABLAS DE RESULTADOS

En el presente anexo de encuentran las tablas de resumen de los datos obtenidos durante el desarrollo del proyecto, en las pruebas realizadas en cada escenario. Éstas fueron utilizadas para los análisis presentados en los capítulos 2 y 3 del Documento Final del Trabajo de Grado y para las conclusiones del mismo.

1. ESCENARIO HOST-HOST

La siguiente tabla contiene los resultados de las pruebas realizadas en modo túnel en el escenario en el que las Asociaciones de Seguridad van de Host a Host.

Para los valores de retardo y variación de retardo sin IPsec en todas las tablas, se realizaron algunas pruebas y se presentan aquí los menores valores obtenidos ya que permiten realizar los análisis cuando la red está funcionando sin ningún contratiempo.

Modo Túnel	Retardo ida (ms)	Variación de retardo ida (ms)	Retardo regreso (ms)	Variación de retardo regreso(ms)
Camellia	1.5 – 2.38	0.63 – 1.8	1.28 – 2.4	5.3 – 6.15
AES	1.05 – 1.87	0.68 – 2.07	0.62 – 0.78	2.84 – 5.3
3DES	0.53 – 0.61	0.66 – 1.56	0.5 – 1.13	2.42 – 7.3
MD5 - Camellia	1.08 – 2.53	1.84 – 4.06	0.57 – 1.35	2.21 – 5.72
SHA - Camellia	0.68 – 0.74	0.62 – 4.18	0.44 – 0.49	3.07 – 5.25
MD5 - AES	2 – 2.53	0.8 – 3.98	0.86 – 1.37	2.88 – 2.98
SHA1 - AES	0.1 – 1.42	0.76 – 5.24	0.28 – 1.1	5 – 5.76
MD5 – 3DES	1.29 – 1.49	3.08 – 8.09	1.25 – 1.41	5.7 – 9.78
SHA – 3DES	0.19 – 1	0.53 – 1.1	1.38 – 2.19	4.08 – 4.38
Sin IPsec	1	1.26	0.55	3.53

Dado que en el escenario se realizaron pruebas en ambos modos de operación de IPsec, la siguiente tabla contiene los resultados de las pruebas realizadas en modo transporte en el escenario Host a Host.

Modo Transporte	Retardo Ida(ms)	Variación de Retardo Ida (ms)	Retardo Regreso (ms)	Variación de Retardo Regreso(ms)
Camellia	2.17 – 2.64	0.8 – 0.83	1.1 – 1.56	2.32 – 5.34
AES	1.04 – 1.33	0.65 – 1.7	0.06 – 0.27	4.5 – 7.37
3DES	0.1 – 1.46	0.5 – 0.58	1 – 2.6	4.05 – 5.75
MD5 - Camellia	0.2 – 0.32	0.5 – 0.51	0.91 – 1.46	0.72 – 5.88
SHA1 - Camellia	0.51 – 0.57	1.88 – 4.12	0.69 – 1.78	3.5 – 5.7
MD5 - AES	0.1 – 0.34	1.37 – 1.88	0.8 – 1.24	2.15 – 4.01
SHA1 - AES	0.18 - 0.39	0.81 - 0.84	0.8 – 0.96	2.51 – 3.82
MD5 – 3DES	1 – 1.82	1.54 – 2.54	0.76 – 0.78	4.92 – 4.96
SHA1 – 3DES	2.3 – 4.91	2.62 – 3.4	2.89 – 3.79	2.66 – 11.73
Sin IPsec	1	1.26	0.55	3.53

2. ESCENARIO SG-SG

La siguiente tabla corresponde a los resultados de las pruebas realizadas en el escenario en el cual las Asociaciones de Seguridad se establecen entre los enrutadores trabajando como Pasarelas de Seguridad, utilizando el protocolo ESP.

ESP	Retardo ida	Variación de Retardo ida	Retardo regreso(ms)	Variación de Retardo regreso
MD5	1.93 - 2	7.58 – 11.8	0.4 – 3.6	0.7 – 3.87
SHA	2.19 – 5.24	6 – 9.68	3.79 – 7	5.69 – 6.1
3DES	6.35 – 6.95	7 – 7.22	8.22 – 8.77	4.59 – 5.69
AES	4.41 – 5.39	6.97 – 8.26	6.15 – 7.14	1.76 - 5
DES	4.82 – 4.83	6.74 – 7.93	6.54 – 6.56	2.134– 3.85
MD5 3DES	12.69 – 20.81	15.5 – 22.5	10.9 – 18.84	14.2 - 17
MD5 AES	6.41 – 6.87	13.58 – 18.6	4.62 – 4.99	2.27 - 4
MD5 DES	4.14 – 9.9	20 – 79.32	2.49 – 7.89	1.7 – 8.45
SHA 3DES	2.19 – 8.14	11 – 23.97	3.74 - 8	3.14 – 7.65
SHA AES	3.61 – 4.39	12 – 15.33	1.82 - 2.53	0.9 – 2.32
SHA DES	4.6 – 6.05	12.31 – 13.5	2.74 – 4.22	0.75 – 2.09
Sin IPsec	1	1.26	0.55	3.53

La siguiente tabla corresponde a los resultados de las pruebas realizadas combinando AH como protocolo de autenticación e integridad y ESP como protocolo de confidencialidad.

AH y ESP	Retardo Ida (ms)	Variación de Retardo Ida (ms)	Retardo Regreso (ms)	Variación de Retardo Regreso(ms)
MD5 3DES	7.31 - 8.73	9.87 - 10.57	9.13 – 10.64	1.13 – 7.66
MD5 AES	7.92 – 13.03	8.34 – 12.37	9.79 – 14.86	1 – 7.5
MD5 DES	7.86 – 8.55	8.32 – 10.48	9.62 – 10.35	2.64 – 5.08
SHA1 3DES	3.64 – 5.27	6.76 – 7.04	5.37 – 7.06	3.2 – 4.94
SHA1 AES	5.93 – 10.47	7.89 – 10.77	7.77 – 12.36	1.89 – 4.58
SHA1 DES	4.89 – 10.52	6.44 – 13.27	6.6 – 12.3	2.67 – 12.8
Sin IPsec	1	1.26	0.55	3.53

3. ESCENARIO HOST-SG

A continuación se presentan los resultados obtenidos de las pruebas del escenario de Host-SG, el cual fue una primera aproximación al escenario siguiente (Acceso Remoto).

Host SG	Retardo (ms)	Variación de Retardo (ms)	Retardo Regreso	Variación de Retardo
MD5 3DES	2.9 – 4.2	6.1 – 6.87	4.16 – 5.6	5.64 – 9.26
AES-MD5	2.39 – 2.95	9.81 – 12.05	3.36 – 4.25	4.99 – 5.76
3DES-SHA1	8.33 – 14.01	10.3 – 25.69	6.89 – 12.43	1.85 – 20.01
AES-SHA1	3.58 – 5.61	13.08 – 16.82	1.92 – 4.15	3.29 – 5.5
Sin IPsec	1	1.26	0.55	3.53

4. ESCENARIO ACCESO REMOTO

La siguiente tabla contiene los resultados de retardo y variación de retardo obtenidos de las pruebas del escenario de Acceso Remoto o Road Warrior.

Host SG	Retardo (ms)	Variación de Retardo (ms)	Retardo Regreso	Variación de Retardo
MD5 3DES	0.88 – 0.97	10.2 – 16.7	1.68 – 2.2	3.62 – 7.37
AES-MD5	4.73 – 5.3	11.7 – 14.6	2.7 – 3.4	3.1 – 4.96
3DES-SHA1	23.5 – 28.3	18.5 – 24.4	21.6 – 26.47	15.2 - 16
AES-SHA1	4.3 – 8.6	5.73 – 15.95	6.15 – 6.75	4.86 – 9.17
Sin IPsec	1	1.26	0.55	3.53

5. ESCENARIO HOST-HOST CON SG-SG

Los resultados de las pruebas realizadas en el escenario Host a Host con SG a SG, que representan SA's iteradas con un túnel entre los Hosts que luego va dentro de otro túnel entre las Pasarelas de Seguridad, se encuentran en la tabla a continuación:

SA entre Hosts	SA entre SGs	Retardo (ms)	Variación de Retardo (ms)	Retardo Regreso	Variación de Retardo
3DES	**AES**	5.13 – 5.37	6.65 – 7.51	7.03 – 7.32	2.25 – 5.94
AES	**3DES MD5**	10.65 – 14.01	11.52 – 11.86	12.69 – 16	5 – 6.1
AES	**3DES SHA**	19.23 – 23.39	11.5 – 13.81	21.27 – 25.4	3.8 - 14
AES SHA	**3DES**	10 - 16	18.2 – 29.5	7.82 - 14	6.31 – 31.7
AES SHA	**MD5 3DES**	10.17 – 13.4	12.6 – 18.48	8 – 11.45	4.8 – 12.18
AES	**3DES**	2.4 – 8.63	9.6 – 14.13	1.2 – 10.65	3.3 – 16.77
AES	**MD5**	5.72 – 13.83	15.5 - 17	8.1 – 15.95	3.4 – 13.73
AES	**SHA**	6.32 – 13.48	9.58 – 20.8	8.3 – 15.7	6 – 13.6
AES MD5	**3DES**	7.22 – 24.63	16.7 – 17.32	5.52 – 22.41	8.1 – 8.52
Sin IPsec		1	1.26	0.55	3.53