

Experiment #1: Impact of Network Bandwidth on Performance

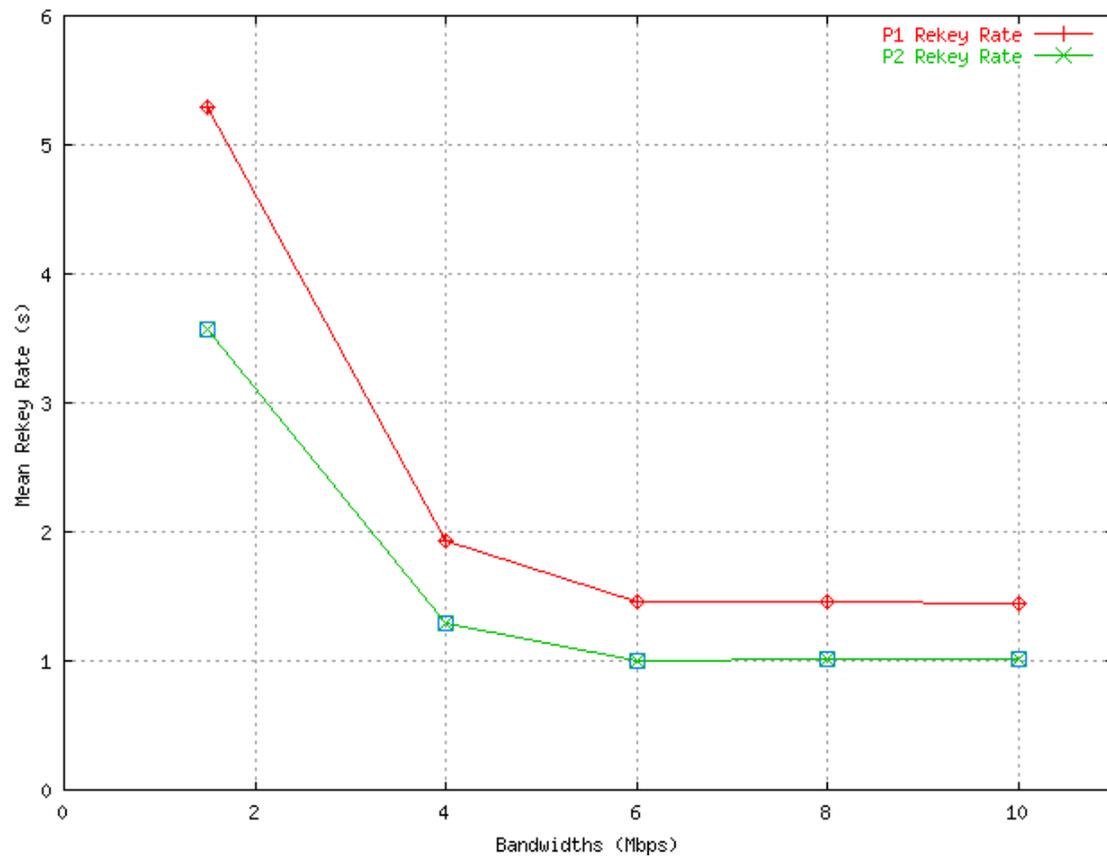


Figure 1: Re-keying Establishment Latency with Various Network Bandwidths

	1.5Mb/s	4Mb/s	6Mb/s	8Mb/s	10Mb/s
Application:					
# of sessions(10MB/ses)	3006	8024	11268	11266	11266
Avg Thrput (kbps)	141.894	389.705	558.711	558.424	558.828
Avg sess.delay (s)	563.802	205.283	143.187	143.26	143.157
# of retransmissions	13	10	10	10	10
IKE: Initiator					
rekeying Sas	203	204	204	204	204
rekeying delay (s)	5.297	1.936	1.453	1.462	1.451
IPSec: Initiator					
rekeying requests	5100	5130	5140	5138	5138
rekeying SA delay (s)	3.567	1.292	1.006	1.009	1.008
pkts dropped (no SAs)	10	10	10	10	10

Table 1: Performance with Various Network Bandwidths

Analysis

As specified in the IPsec specification, IKE SA set-up requires 6 messages (3 round trips) and 3 messages for IPsec SA set-up (i.e., requires 2 round trips including either an optional Delete message or user traffic with the new SA) for the SA initiator.

Figure 1 shows the re-key establishment latency with various network bandwidths. Table 1 presents the relative performance data, with varying network bandwidths, relative to SA re-keying latency, TCP application throughput and delay.

Assuming the processors provide sufficient processing power to fully utilize the underlying link capacity except for cryptographic processing, the relative IPsec performance (e.g., SA re-keying delay), as shown in Figure 1, tends to be increasing as network bandwidth increases at security gateways. Specifically, in this experiment, the performance of SA re-keying latency seems to be increasing greatly when used with network bandwidth of up to 6Mb/s. From this point, the Figure shows, the performance of IPsec seems to be stable, independent of network capacity. The performance of TCP applications shows the same performance characteristics as that of IPsec, as shown in Table 1. This seems to indicate that the cryptographic performance seems to become the bottleneck of the overall system performance when used with network capacity of higher than 6Mb/s in this experiment.

With the current traffic load, the maximum IPsec performance tends to have reached when used with the NIC capacity of a little over 6Mb/s, as shown Table 1 above. Note that these results are relevant to the cryptographic performance and traffic load provided for the experiment.

Initial TCP SYN segments from the FTP clients (e.g., 10 TCP clients here) seemed to be dropped at the gateway and retransmitted by the application clients. For the case of 1.5Mb/s, there also occur a number of retransmissions of a FIN segment.

It seems to indicate that, when all other conditions are equal, the best IPsec performance of a security gateway can be achieved when it maintains the network bandwidth capacity of equal or higher than the rate of overall cryptographic processing. In other words, if network connection provides enough capacity to handle the maximum cryptographic performance, then the cryptographic performance seems to become the bottleneck of the overall system performance, independent of network capacity. However, if network connection does not meet the rate of overall cryptographic processing of a security system, then, the network capacity becomes the bottleneck of the overall system performance.